UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT, INC., Plaintiffs v. FORCEPOINT LLC, Defendant.	CIVIL ACTION NO. 6:22-CV-00342 **JURY TRIAL DEMANDED**
FORCEPOINT LLC, Counterclaim Plaintiff, v. WEBROOT, INC., OPEN TEXT, INC., and OPEN TEXT CORPORATION Counterclaim-Defendants.	

DEFENDANT FORCEPOINT LLC'S FIRST AMENDED ANSWER AND COUNTERCLAIMS TO PLAINTIFFS' COMPLAINT FOR PATENT INFRINGEMENT

Defendant Forcepoint LLC ("Forcepoint" or "Defendant"), by and through its undersigned counsel, answers Plaintiffs Webroot, Inc.'s ("Webroot") and Open Text Inc.'s (collectively, "Plaintiffs") Complaint for Patent Infringement (the "Complaint"), dated March 31, 2022. All allegations, including those contained in the headings of the Complaint, not expressly admitted herein are denied by Forcepoint.

Forcepoint's specific responses to the numbered allegations of the Complaint are in the below numbered paragraphs as follows:

1. Forcepoint denies that any of the Asserted Patents "helped to revolutionize and have become widely adopted in, the fields of malware detection, network security, and endpoint protection." Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 1 and therefore denies them.

2. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 2 and therefore denies them.

3. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 3 and therefore denies them.

4. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 4 and therefore denies them.

5. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 5 and therefore denies them.

6. Forcepoint denies the allegations of paragraph 6 of the Complaint.

7. Forcepoint denies the allegations of paragraph 7 of the Complaint.

8. To the extent the allegations in paragraph 8 purport to describe what is in the Asserted Patents, Forcepoint asserts that the Asserted Patents speak for themselves. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 8 and therefore denies them.

9. Forcepoint denies the allegations of paragraph 9 of the Complaint.

10. Forcepoint denies the allegations of paragraph 10 of the Complaint.

11. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 11 and therefore denies them.

12. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 12 and therefore denies them.

13. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 13 and therefore denies them.

14. Forcepoint denies the allegations of paragraph 14 of the Complaint.

15. Forcepoint admits that it markets certain products and services named "Next-Generation Firewall, Web Appliance or Secure Web Gateway, Web Security, Forcepoint One, Advanced Classification Engine, Threat Seeker Intelligence, Advance Malware Detection, and Remote Browser Isolation." Forcepoint denies the remaining allegations in paragraph 15 of the Complaint, and specifically denies that Forcepoint "implements Plaintiffs' patent technology" and denies that Forcepoint has committed any acts of infringement.

16. Forcepoint admits that the Complaint purports "to seek damages for and to ultimately stop Defendant's continued infringement of Plaintiffs' patents." Forcepoint denies the remaining allegations contained in paragraph 16, including that Forcepoint committed any acts of "infringement of Plaintiffs' patents" or engaged in "unlawful competition."

NATURE OF THE CASE[1]

17. Forcepoint admits that the Complaint purports to allege patent infringement under the patent laws of the United States, Title 35 of the United States Code. Forcepoint denies the remaining allegations in paragraph 17, including that it "has infringed and continue[s] to infringe" any of Plaintiffs' patents.

[1] For ease of reference, Forcepoint adopts the headings set forth in the Complaint. To the extent that such headings themselves contain factual or legal characterizations or allegations, Forcepoint denies such characterizations and allegations.

THE PARTIES

18. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 18 and therefore denies them.

19. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 19 and therefore denies them.

20. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 20 and therefore denies them.

21. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 21 and therefore denies them.

22. Forcepoint a lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 22 and therefore denies them.

23. Forcepoint admits that it is a Delaware limited liability company with a principal place of business at 10900-A Stonelake Blvd #350, Austin, TX 78759. Forcepoint admits that it is registered with the Secretary of State to conduct business in Texas. Forcepoint denies the remaining allegations contained in paragraph 23.

JURISDICTION & VENUE

24. Forcepoint admits that the Complaint purports to set forth patent infringement claims arising under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*. Forcepoint admits that this Court has subject matter jurisdiction over actions arising under the patent laws of the United States pursuant to 28 U.S.C. §§ 1331 and 1338(a). Forcepoint denies the remaining allegations contained in paragraph 24.

25. Forcepoint admits that its principal place of business is located in the state of Texas. Forcepoint admits that it has conducted business in the State of Texas and in the Western

District of Texas. For the purposes of only this case, Forcepoint does not contest personal jurisdiction. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer. Forcepoint denies the remaining allegations contained in paragraph 25, including that it has committed any acts of infringement.

26. Forcepoint admits that it sells products that may be used nationwide, including in the Western District of Texas. Forcepoint denies the remaining allegations in paragraph 26, including that its products infringe any of Plaintiffs' patents. To the extent the allegations in paragraph 26 purport to describe what is in documents (*e.g.*, Forcepoint, *Find a Partner*, https://www.forcepoint.com/partners/find-a-partner), Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

27. Forcepoint admits that venue is proper in the Western District of Texas for purposes of only this action, but denies that venue is convenient or in the interest of justice under 28 U.S.C. § 1404(a). Forcepoint denies the remaining allegations in paragraph 27, including that it has committed any acts of infringement.

28. Forcepoint admits it has employees in Austin, Texas with relevant knowledge regarding the Accused Products. Forcepoint denies the remaining allegations of paragraph 28.

29. Forcepoint admits it has employees in Austin, Texas with knowledge regarding sales and support of the Accused Products. Forcepoint denies the remaining allegations of paragraph 29.

30. Forcepoint admits it uses aspects of certain of its products in Austin, Texas, but denies that any such use is an act of infringement of any claim of the Asserted Patents.

Forcepoint specifically denies that it has committed any acts of infringement in this District or otherwise. Forcepoint denies the remaining allegations of paragraph 30.

31. Forcepoint admits it sells, offers for sale, and advertises its products nationwide, including in the Western District of Texas, but denies that it has committed any acts of infringement in this District or otherwise. Forcepoint denies the remaining allegations in paragraph 31 of the Complaint, including that it has committed any acts of infringement.

32. Forcepoint denies the allegations in paragraph 32 of the Complaint. To the extent the allegations in paragraph 32 purport to describe what is in documents (*e.g.*, Forcepoint, *Find a Partner*, https://www.forcepoint.com/partners/find-a-partner), Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

33. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer. Forcepoint denies the remaining allegations in paragraph 33 of the Complaint.

34. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer. Forcepoint denies the remaining allegations in paragraph 34 of the Complaint.

35. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer. Forcepoint denies the remaining allegations in paragraph 35 of the Complaint. To the extent the allegations in paragraph 35 purport to describe what is in documents (*e.g.*, Forcepoint, *Welcome to Forcepoint Hub*, https://support.forcepoint.com/s/login/?ec=302&startURL=%2Fs%2F),

Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

36. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer. Forcepoint denies the allegations in paragraph 36 of the Complaint.

37. Forcepoint denies the allegations in paragraph 37 of the Complaint.

PLAINTIFFS' PATENTED INNOVATIONS

38. Forcepoint denies that Plaintiffs and their predecessors "were all pioneers and leading innovators in developing and providing modern end point security protection." Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 38 and therefore denies them.

39. Forcepoint denies that the Asserted Patents reflect "innovations" or "improve on traditional anti-Malware and network security systems." Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 39 and therefore denies them.

U.S. Patent No. 8,726,389

40. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 40 and therefore denies them.

41. Forcepoint admits that what appears to be a copy United States Patent No. 8,726,389 is attached as Exhibit 1 to the complaint and that, on its face, the '389 Patent is entitled "Methods and Apparatus for Dealing with Malware" and bears the filing date of July 8,

2012. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 41 and therefore denies them.

42. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 42 and therefore denies them.

43. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 43 and therefore denies them.

44. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 44 and therefore denies them.

45. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 45 and therefore denies them.

46. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 46 and therefore denies them.

47. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information

sufficient to form a belief as to the truth of the allegations of paragraph 47 and therefore denies them.

48. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 48 and therefore denies them.

49. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 49 and therefore denies them.

50. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 50 and therefore denies them.

51. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 51 and therefore denies them.

52. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 52 and therefore denies them.

53. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 53 and therefore denies them.

54. Forcepoint admits that Plaintiffs purport to characterize the '389 Patent, but asserts that the '389 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 54 and therefore denies them.

U.S. Patent No. 10,599,844

55. Forcepoint admits that what appears to be a copy United States Patent No. 10,599,844 is attached as Exhibit 2 to the complaint and that, on its face, the '844 Patent is entitled "Automatic Threat Detection of Executable Files Based on Static Data Analysis" and bears the filing date of May 12, 2015. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 55 and therefore denies them.

56. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 56 and therefore denies them.

57. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 57 and therefore denies them.

58. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 58 and therefore denies them.

59. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 59 and therefore denies them.

60. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 60 and therefore denies them.

61. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 61 and therefore denies them.

62. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 62 and therefore denies them.

63. Forcepoint admits that Plaintiffs purport to characterize the '844 Patent, but asserts that the '844 Patent speaks for itself. Forcepoint lacks knowledge or information

sufficient to form a belief as to the truth of the allegations of paragraph 63 and therefore denies them.

U.S. Patent No. 8,438,386

64. Forcepoint admits that what appears to be a copy United States Patent No. 8,438,386 is attached as Exhibit 3 to the complaint and that, on its face, the '386 Patent is entitled "System and Method for Developing a Risk Profile for an Internet Service" and bears the filing date of February 21, 2010. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 55 and therefore denies them.

65. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 65 and therefore denies them.

66. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 66 and therefore denies them.

67. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 67 and therefore denies them.

68. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information

sufficient to form a belief as to the truth of the allegations of paragraph 68 and therefore denies them.

69. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 69 and therefore denies them.

70. Forcepoint admits that Plaintiffs purport to characterize the '386 Patent, but asserts that the '386 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 70 and therefore denies them.

U.S. Patent No. 9,413,721

71. Forcepoint admits that what appears to be a copy United States Patent No. 9,413,721 is attached as Exhibit 4 to the complaint and that, on its face, the '721 Patent is entitled "Methods and Apparatus for Dealing with Malware" and bears the filing date of February 13, 2012. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 55 and therefore denies them.

72. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 72 and therefore denies them.

73. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information

sufficient to form a belief as to the truth of the remaining allegations of paragraph 73 and therefore denies them.

74. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 74 and therefore denies them.

75. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 75 and therefore denies them.

76. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 76 and therefore denies them.

77. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 77 and therefore denies them.

78. Forcepoint admits that Plaintiffs purport to characterize the '721 Patent, but asserts that the '721 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 78 and therefore denies them.

U.S. Patent No. 10,025,928

79. Forcepoint admits that what appears to be a copy United States Patent No. 10,025,928 is attached as Exhibit 5 to the complaint and that, on its face, the '928 Patent is entitled "Proactive Browser Content Analysis" and bears the filing date of October 3, 2012. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 79 and therefore denies them.

80. Forcepoint admits that Plaintiffs purport to characterize the '928 Patent, but asserts that the '928 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 80 and therefore denies them.

81. Forcepoint admits that Plaintiffs purport to characterize the '928 Patent, but asserts that the '928 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 81 and therefore denies them.

82. Forcepoint admits that Plaintiffs purport to characterize the '928 Patent, but asserts that the '928 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 82 and therefore denies them.

83. Forcepoint admits that Plaintiffs purport to characterize the '928 Patent, but asserts that the '928 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 83 and therefore denies them.

84. Forcepoint admits that Plaintiffs purport to characterize the '928 Patent, but asserts that the '928 Patent speaks for itself. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 84 and therefore denies them.

ACCUSED PRODUCTS

85. Forcepoint admits that it markets certain products and services named "Next-Generation Firewall, Web Appliance, Web Security or Secure Web Gateway, Advanced Classification Engine, Threat Seeker Intelligence, Advance Malware Detection, Forcepoint One, and Remote Browser Isolation." Forcepoint denies the remaining allegations of paragraph 85, including that any of its products, in combination or individually, infringe any of Plaintiffs' patents.

86. Forcepoint denies the allegations in paragraph 86. To the extent the allegations in paragraph 86 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

87. Forcepoint denies the allegations in paragraph 87. To the extent the allegations in paragraph 87 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

88. Forcepoint denies the allegations in paragraph 88. To the extent the allegations in paragraph 88 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

89. Forcepoint denies the allegations in paragraph 89. To the extent the allegations in paragraph 89 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

90. Forcepoint denies the allegations in paragraph 90. To the extent the allegations in paragraph 90 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

91. Forcepoint denies the allegations in paragraph 91. To the extent the allegations in paragraph 91 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

92. Forcepoint denies the allegations in paragraph 92. To the extent the allegations in paragraph 92 purport to describe what is in documents, Forcepoint asserts that those documents speak for themselves. Forcepoint denies the allegations to the extent they do not accurately represent the documents.

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE '389 PATENT)

93. Forcepoint incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

94. Forcepoint denies the allegations in paragraph 94 of the Complaint.

95. Forcepoint admits that what appears to be claim 1 of the '389 Patent is recited at paragraph 95 of the Complaint. Forcepoint denies the remaining allegations of paragraph 95.

96. Forcepoint denies the allegations in paragraph 96 of the Complaint.

97. Forcepoint denies the allegations in paragraph 97 of the Complaint.

98. Forcepoint denies the allegations in paragraph 98 of the Complaint.

99. Forcepoint denies the allegations in paragraph 99 of the Complaint.

100. Forcepoint denies the allegations in paragraph 100 of the Complaint.

101. Forcepoint denies the allegations in paragraph 101 of the Complaint.

102. Forcepoint denies the allegations in paragraph 102 of the Complaint.

103. Forcepoint denies the allegations in paragraph 103 of the Complaint.

104. Forcepoint denies the allegations in paragraph 104 of the Complaint.

105. Forcepoint denies the allegations in paragraph 105 of the Complaint.

106. Forcepoint admits it was notified of the '389 Patent at the time it was served with the Complaint, but denies that the Complaint provides information sufficient to allege a plausible claim of infringement of any claim of the '389 Patent. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 106 and therefore denies them.

107. Forcepoint denies the allegations in paragraph 107 of the Complaint.

108. Forcepoint denies the allegations in paragraph 108 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

109. Forcepoint denies the allegations in paragraph 109 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

110. Forcepoint denies the allegations in paragraph 110 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

111. Forcepoint denies the allegations in paragraph 111 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

112. Forcepoint denies the allegations in paragraph 112 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

113. Forcepoint denies the allegations in paragraph 113 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

114. Forcepoint denies the allegations in paragraph 114 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

115. Forcepoint denies the allegations in paragraph 115 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

116. Forcepoint denies the allegations in paragraph 116 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

117. Forcepoint denies the allegations in paragraph 117 of the Complaint.

118. Forcepoint denies the allegations in paragraph 118 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

119. Forcepoint denies the allegations in paragraph 119 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

120. Forcepoint incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

121. Forcepoint denies the allegations in paragraph 121 of the Complaint.

122. Forcepoint admits that what appears to be claim 1 of the '844 Patent is recited at paragraph 122 of the Complaint. Forcepoint denies the remaining allegations of paragraph 122.

123. Forcepoint denies the allegations in paragraph 123 of the Complaint.

124. Forcepoint denies the allegations in paragraph 124 of the Complaint.

125. Forcepoint denies the allegations in paragraph 125 of the Complaint.

126. Forcepoint denies the allegations in paragraph 126 of the Complaint.

127. Forcepoint denies the allegations in paragraph 127 of the Complaint.

128. Forcepoint denies the allegations in paragraph 128 of the Complaint.

129. Forcepoint denies the allegations in paragraph 129 of the Complaint.

130. Forcepoint denies the allegations in paragraph 130 of the Complaint.

131. Forcepoint denies the allegations in paragraph 131 of the Complaint.

132. Forcepoint admits it was notified of the '844 Patent at the time it was served with the Complaint, but denies that the Complaint provides information sufficient to allege a plausible

claim of infringement of any claim of the '844 Patent. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 132 and therefore denies them.

133. Forcepoint denies the allegations in paragraph 133 of the Complaint.

134. Forcepoint denies the allegations in paragraph 134 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

135. Forcepoint denies the allegations in paragraph 135 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

136. Forcepoint denies the allegations in paragraph 136 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

137. Forcepoint denies the allegations in paragraph 137 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

138. Forcepoint denies the allegations in paragraph 138 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

139. Forcepoint denies the allegations in paragraph 139 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

140. Forcepoint denies the allegations in paragraph 140 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

141. Forcepoint denies the allegations in paragraph 141 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

142. Forcepoint denies the allegations in paragraph 142 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

143. Forcepoint denies the allegations in paragraph 143 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

144. Forcepoint denies the allegations in paragraph 144 of the Complaint.

145. Forcepoint denies the allegations in paragraph 145 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

146. Forcepoint denies the allegations in paragraph 146 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

147. Forcepoint denies the allegations in paragraph 147 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

148. Forcepoint denies the allegations in paragraph 148 of the Complaint.

149. Forcepoint denies the allegations in paragraph 149 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

150. Forcepoint denies the allegations in paragraph 150 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

151. Forcepoint denies the allegations in paragraph 151 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE '386 PATENT)

152. Forcepoint incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

153. Forcepoint denies the allegations in paragraph 153 of the Complaint.

154. Forcepoint admits that what appears to be claim 1 of the '386 Patent is recited at paragraph 154 of the Complaint. Forcepoint denies the remaining allegations of paragraph 154.

155. Forcepoint denies the allegations in paragraph 155 of the Complaint.

156. Forcepoint denies the allegations in paragraph 156 of the Complaint.

157. Forcepoint denies the allegations in paragraph 157 of the Complaint.

158. Forcepoint denies the allegations in paragraph 158 of the Complaint.

159. Forcepoint denies the allegations in paragraph 159 of the Complaint.

160. Forcepoint denies the allegations in paragraph 160 of the Complaint.

161. Forcepoint denies the allegations in paragraph 161 of the Complaint.

162. Forcepoint denies the allegations in paragraph 162 of the Complaint.

163. Forcepoint admits it was notified of the ’386 Patent at the time it was served with the Complaint, but denies that the Complaint provides information sufficient to allege a plausible claim of infringement of any claim of the ’386 Patent. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 163 and therefore denies them.

164. Forcepoint denies the allegations in paragraph 164 of the Complaint.

165. Forcepoint denies the allegations in paragraph 165 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

166. Forcepoint denies the allegations in paragraph 166 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

167. Forcepoint denies the allegations in paragraph 167 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

168. Forcepoint denies the allegations in paragraph 168 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

169. Forcepoint denies the allegations in paragraph 169 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

170. Forcepoint denies the allegations in paragraph 170 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

171. Forcepoint denies the allegations in paragraph 171 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

172. Forcepoint denies the allegations in paragraph 172 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

173. Forcepoint denies the allegations in paragraph 173 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

174. Forcepoint denies the allegations in paragraph 174 of the Complaint.

175. Forcepoint denies the allegations in paragraph 175 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

176. Forcepoint denies the allegations in paragraph 176 of the Complaint.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE '721 PATENT)

177. Forcepoint incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

178. Forcepoint denies the allegations in paragraph 178 of the Complaint.

179. Forcepoint admits that what appears to be claim 1 of the '721 Patent is recited at paragraph 179 of the Complaint. Forcepoint denies the remaining allegations of paragraph 179.

180. Forcepoint denies the allegations in paragraph 180 of the Complaint.

181. Forcepoint denies the allegations in paragraph 181 of the Complaint.

182. Forcepoint denies the allegations in paragraph 182 of the Complaint.

183. Forcepoint denies the allegations in paragraph 183 of the Complaint.

184. Forcepoint denies the allegations in paragraph 184 of the Complaint.

185. Forcepoint denies the allegations in paragraph 185 of the Complaint.

186. Forcepoint denies the allegations in paragraph 186 of the Complaint.

187. Forcepoint denies the allegations in paragraph 187 of the Complaint.

188. Forcepoint denies the allegations in paragraph 188 of the Complaint.

189. Forcepoint denies the allegations in paragraph 189 of the Complaint.

190. Forcepoint admits it was notified of the '721 Patent at the time it was served with the Complaint, but denies that the Complaint provides information sufficient to allege a plausible claim of infringement of any claim of the '721 Patent. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 190 and therefore denies them.

191. Forcepoint denies the allegations in paragraph 191 of the Complaint.

192. Forcepoint denies the allegations in paragraph 192 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

193. Forcepoint denies the allegations in paragraph 193 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

194. Forcepoint denies the allegations in paragraph 194 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

195. Forcepoint denies the allegations in paragraph 195 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

196. Forcepoint denies the allegations in paragraph 196 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

197. Forcepoint denies the allegations in paragraph 197 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

198. Forcepoint denies the allegations in paragraph 198 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

199. Forcepoint denies the allegations in paragraph 199 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

200. Forcepoint denies the allegations in paragraph 200 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

201. Forcepoint denies the allegations in paragraph 201 of the Complaint.

202. Forcepoint denies the allegations in paragraph 202 of the Complaint.

203. Forcepoint denies the allegations in paragraph 203 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE '928 PATENT)

204. Forcepoint incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

205. Forcepoint denies the allegations in paragraph 205 of the Complaint.

206. Forcepoint admits that what appears to be claim 1 of the '928 Patent is recited at paragraph 206 of the Complaint. Forcepoint denies the remaining allegations of paragraph 206.

207. Forcepoint denies the allegations in paragraph 207 of the Complaint.

208. Forcepoint denies the allegations in paragraph 208 of the Complaint.

209. Forcepoint denies the allegations in paragraph 209 of the Complaint.

210. Forcepoint denies the allegations in paragraph 210 of the Complaint.

211. Forcepoint denies the allegations in paragraph 211 of the Complaint.

212. Forcepoint denies the allegations in paragraph 212 of the Complaint.

213. Forcepoint denies the allegations in paragraph 213 of the Complaint.

214. Forcepoint denies the allegations in paragraph 214 of the Complaint.

215. Forcepoint denies the allegations in paragraph 215 of the Complaint.

216. Forcepoint denies the allegations in paragraph 216 of the Complaint.

217. Forcepoint denies the allegations in paragraph 217 of the Complaint.

218. Forcepoint denies the allegations in paragraph 218 of the Complaint.

219. Forcepoint admits it was notified of the '928 Patent at the time it was served with the Complaint, but denies that the Complaint provides information sufficient to allege a plausible

claim of infringement of any claim of the '928 Patent. Forcepoint lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of paragraph 219 and therefore denies them.

220. Forcepoint denies the allegations in paragraph 220 of the Complaint.

221. Forcepoint denies the allegations in paragraph 221 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

222. Forcepoint denies the allegations in paragraph 222 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

223. Forcepoint denies the allegations in paragraph 223 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

224. Forcepoint denies the allegations in paragraph 224 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

225. Forcepoint denies the allegations in paragraph 225 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

226. Forcepoint denies the allegations in paragraph 226 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

227. Forcepoint denies the allegations in paragraph 227 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

228. Forcepoint denies the allegations in paragraph 228 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

229. Forcepoint denies the allegations in paragraph 229 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

230. Forcepoint denies the allegations in paragraph 230 of the Complaint.

231. Forcepoint denies the allegations in paragraph 231 of the Complaint.

232. Forcepoint denies the allegations in paragraph 232 of the Complaint. Plaintiffs dismissed their allegations in the Complaint as to pre-suit indirect infringement (Dkt. 20), and thus, Forcepoint does not respond to those allegations in its Answer.

PRAYER FOR RELIEF

The Complaint recites a prayer for relief for which no response is required. To the extent an answer is required, Forcepoint denies that Plaintiffs are entitled to any relief.

DEMAND FOR JURY TRIAL

The Complaint sets forth Plaintiffs' jury demand and requires no response. To the extent an answer is required, Forcepoint admits that the Complaint contains a request for jury trial but denies that Plaintiffs are entitled to any relief.

AFFIRMATIVE DEFENSES/DEFENSES

1. Without any admission that Forcepoint bears the burden of proof, burden of persuasion, or the truth of any allegation in the Complaint, Forcepoint relies on the following defenses, whether pled as an affirmative defense or otherwise, in response to the allegations, which are based on an investigation that is not complete.

FIRST DEFENSE
(Non-infringement)

2. Forcepoint does not infringe, and at all relevant times to this action has not infringed, directly or indirectly, literally or under the Doctrine of Equivalents, any valid and enforceable claim of the Asserted Patents.

SECOND DEFENSE
(Invalidity)

3. The claims of the Asserted Patents are invalid for failure to satisfy one or more of the conditions and requirements of patentability set forth in 35 U.S.C. §§ 101 et seq., including, but not limited to, 35 U.S.C. §§ 101, 102, 103, 112, and/or 116, or under any of the judicially created doctrines of invalidity.

THIRD DEFENSE
(Failure To State a Claim)

4. The Complaint fails to state a claim on which relief can be granted.

FOURTH DEFENSE
(Prosecution History Estoppel)

5. Plaintiffs are estopped from construing any valid and enforceable claim of the Asserted Patents to cover or include, either literally or by application of the doctrine of equivalents, devices manufactured, used, imported, sold, offered for sale, or imported by Forcepoint, or methods used by Forcepoint, because of admissions and statements to the United

States Patent and Trademark Office during prosecution of the applications leading to the issuance of the Asserted Patents or applications related thereto, because of disclosures or language in the specifications of the Asserted Patents, and/or limitations in the claims of the Asserted Patents.

FIFTH DEFENSE
(License and/or Patent Exhaustion)

6. Plaintiffs' claims are barred, in whole or in part, under the doctrines of express license, implied license, and/or patent exhaustion.

SIXTH DEFENSE
(Limitations on Damages)

7. Plaintiffs' claims for damages for alleged patent infringement, if any, are limited by 35 U.S.C. §§ 286, 287, and 288.

SEVENTH DEFENSE
(Remedy by Action Against the United States)

8. Plaintiffs' claims for relief and prayer for damages are limited by 28 U.S.C. § 1498(a).

EIGHTH DEFENSE
(Consent, Waiver, and Estoppel)

9. Plaintiffs' claims are barred, in whole or in part, by consent, waiver and/or estoppel.

NINTH DEFENSE
(Unclean Hands)

10. Plaintiffs' claims are barred by the doctrine of unclean hands.

TENTH DEFENSE
(No Irreparable Harm)

11. Plaintiffs are not entitled to any form of injunctive relief because Plaintiffs have not suffered and will not suffer irreparable harm due to Forcepoint's alleged infringement and because Plaintiffs have an adequate remedy at law.

ADDITIONAL DEFENSES

12. Forcepoint expressly reserves the right to raise and allege additional defenses pursuant to Rule 8 of the Federal Rules of Civil Procedure, the patent laws of the United States, and any other defenses at law or in equity, that may exist or in the future may be available based on further investigation and discovery.

DEMAND FOR JURY TRIAL

13. Forcepoint requests a jury trial on issues so triable by right.

REQUEST FOR RELIEF

WHEREFORE, Defendant Forcepoint respectfully requests that the Court enter judgment in its favor and against Plaintiffs as follows:

A. Dismissing, with prejudice, Plaintiffs' claims against Forcepoint;

B. Denying all relief that Plaintiffs seek in the Complaint;

C. Finding this case to be exceptional under 35 U.S.C. § 285 and awarding Forcepoint its costs and attorneys' fees; and

D. Awarding any other relief the Court deems just and equitable.

FORCEPOINT'S COUNTERCLAIMS

In accordance with Rule 13 of the Federal Rules of Civil Procedure, Forcepoint, Inc. ("Forcepoint" or "Counterclaim-Plaintiff") hereby alleges and asserts the following counterclaims against Open Text, Inc. and Open Text Corporation ("Open Text Corp.") (hereinafter, collectively as "OpenText"), and Webroot, Inc. ("Webroot") (collectively, "Counterclaim-Defendants"), Open Text Corp. being joined pursuant to Rule 20(a)(2) of the Federal Rules of Civil Procedure:

PARTIES

1. Forcepoint is a corporation organized under the laws of Delaware with its corporate headquarters at 10900-A Stonelake Blvd., Quarry Oaks 1, Ste 350, Austin, TX 78759.

2. Webroot is a Delaware corporation with its principal place of business at 385 Interlocken Crescent, Ste 800, Broomfield, CO 80021.

3. Open Text, Inc. is a Delaware corporation with its principal place of business at 2440 Sand Hill Road, Ste 301 & 302, Menlo Park, CA 94025.

4. Open Text Corp. is a Canadian corporation with its principal place of business at 275 Frank Tompa Drive, Waterloo, Ontario, Canada N2L 0A1.

5. Webroot and Open Text, Inc. are subsidiaries of Open Text Corp., a publicly traded company.

JURISDICTION AND VENUE

6. Forcepoint's counterclaims arise under the patent laws of the United States, Title 35 of the United States Code, and the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*.

7. This Court has subject matter jurisdiction over these counterclaims pursuant to 28 U.S.C. §§ 1331, 1338, 2201, and 2202.

8. The Court has personal jurisdiction over Open Text Corp., Open Text, Inc., and Webroot at least because they regularly conducts business in the State of Texas and in this District, including making, using, offering to sell, selling, or importing products and/or services that infringe one or more claims of the Asserted Patents.

9. Open Text Corp. has, either directly or indirectly through its partners, purposefully and voluntarily placed one or more of its infringing products and/or services into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, including, for example, OpenText Documentum. *Open Text Corp. v. Alfresco Software, Ltd.*, No. 6:20-cv-00941, Dkt. No. 1 (Complaint) ¶¶ 3-6 (W.D. Tex. Oct. 9, 2020).

10. Open Text Corp. and Open Text Inc. maintain three offices in the State of Texas, two of which are located in this Judicial District, including the Austin office and San Antonio office. *Id.* ¶ 9; *see also* Dkt. 1, ¶ 22.

11. Over 60 employees work in OpenText's Austin office, including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. *Open Text Corp.*, No. 6:20-cv-00941, Dkt. No. 1 (Complaint) ¶ 9; *see also* Dkt. 1, ¶ 22.

12. OpenText's Austin office hosts one of OpenText's data centers. *Open Text Corp.*, No. 6:20-cv-00941, Dkt. No. 1 (Complaint) ¶ 9; *see also* Dkt. 1, ¶ 22.

13. Webroot and Open Text, Inc. have consented to personal jurisdiction of this Court at least by commencing its action against Forcepoint in this Court. Additionally, Open Text Inc. alleges in its Complaint that it is registered to do business in the State of Texas." Dkt. 1, ¶ 21. Webroot also alleges that it "is a registered business in Texas with multiple customers in this

District" and that it "partners with several entities in this District to resell, distribute, install, and consult on Webroot's products." *Id.*, ¶ 20.

14. Webroot operates out of OpenText's Austin, Texas office. For example, an OpenText job posting for a software developer position located in Austin, Texas states that "Carbonite and Webroot form the SMB and Consumer Division of OpenText" and discusses job duties for the "Webroot Integration team." *See, e.g.,* Ex. 26 (https://www.linkedin.com/jobs/view/software-developer-usa-at-opentext-3139106879/, last accessed July 14, 2022).

15. As another example, OpenText Security Solutions account executive Jim Barry states that he works in Austin, Texas for OpenText, "Carbonite + Webroot," and his job duties consist of "growth within the Carbonite and Webroot product portfolios." *See, e.g.*, Ex. 27 (https://www.linkedin.com/in/jim-barry-295b8ba6/, last accessed July 14, 2022).

16. Webroot conducts business in this District through partners including, for example, ComputerSolution Technology Services located Waco, Texas. ComputerSolution Technology Services has been "providing computer support to . . . McClennan County for almost a decade" and "partner[s] with Webroot to provide business-class endpoint protection with **Secure*Anywhere***." *See, e.g.*, Ex. 28 (https://www.computersolution.tech/, last accessed July 14, 2022) at 1, 8; s*ee also* https://www.computersolution.tech//endpoint-protection/, last accessed July 14, 2022.

17. Venue is proper in this District as to these Counterclaims against Webroot and Open Text, Inc. pursuant to 28 U.S.C. §§ 1391(a)-(c), and 1400(b) at least because Webroot and Open Text, Inc. have consented to the venue of this Court by filing its Complaint here and

because Webroot and Open Text, Inc. have regular and established place of business in this District.

18. Venue is proper in this District as to these Counterclaims against Open Text Corp. pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because Open Text Corp. is a foreign corporation and may be sued in any district in the United States, including this District.

BACKGROUND

Forcepoint

19. Since its inception in 1996, Forcepoint has been the leader in user and data protection cybersecurity, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

20. Previously known as Websense, Inc., Forcepoint has evolved through a strategic focus on top-of-the line technologies that anticipate customers' needs and ensure customers' data is protected. Forcepoint's innovative technologies safeguard over 14,500 companies in over 150 countries around the world in a wide range of industries, including government, finance, energy, infrastructure, and healthcare.

21. For over two decades, Forcepoint has spent 100s of millions of dollars on research and development in security technologies. Today, Forcepoint has over 2,500 employees worldwide, with over 700 employees specifically focused on engineering and research and development.

22. Forcepoint's pioneering Internet security, data security, and email security technologies have also repeatedly been recognized by the United States Patent & Trademark Office, which has awarded Forcepoint hundreds of patents. These patents include U.S. Patent

Nos. 7,194,464; 8,938,773; 8,978,140; 9,609,101; and 9,654,495 (collectively, the "Asserted Counterclaim Patents").

OpenText and Webroot

23. OpenText and Webroot's story is different. Years after its founding, after struggling to compete in the marketplace, Webroot decided to hire away Forcepoint's senior engineers to lead its threat intelligence development, including engineers named on patents Webroot now asserts against Forcepoint in its Complaint. For example, Webroot hired Forcepoint's (then Websense's) Vice President of Engineering Ron Hegli to serve as its CTO of Hosted Security. Hal Lonas, another inventor on Webroot's Asserted Patents, previously was Forcepoint's (then Websense's) Director of Engineering and later became Webroot's and OpenText's CTO.

24. As a result, although OpenText and Webroot assert that Forcepoint is infringing their patents, they are in fact relying on foundational Forcepoint technology across their business lines. As detailed below, OpenText and Webroot built their products and services by infringing Forcepoint's patented technology without justification. OpenText and Webroot's improper use of Forcepoint's technologies has not only caused harm to Forcepoint, as alleged below, but has also harmed innovation in the industry as a whole and encouraged other companies to freely use others' patented technologies. Forcepoint thus requests injunctive relief to stop OpenText and Webroot's improper infringement of Forcepoint's patents.

COUNTERCLAIM-DEFENDANTS' ACCUSED PRODUCTS

25. Webroot and OpenText offer security software and services that implement Forcepoint's patented technologies including, but not limited to, BrightCloud Threat Intelligence

Services, Webroot DLP, Webroot DNS Protection, and OpenText Documentum (the "Counterclaim-Defendants' Accused Products").

FORCEPOINT'S PATENTS

U.S. Patent No. 7,194,464

26. On March 20, 2007, the United States Patent and Trademark Office (the "USPTO") issued U.S. Patent No. 7,194,464 (the "'464 Patent"), titled "System and Method for Adapting An Internet Filter." The '464 Patent is valid and enforceable. A copy of the '464 Patent is attached as Exhibit 1.

27. Forcepoint is the owner of all rights, title, and interest in and to the '464 Patent, and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '464 Patent.

28. The '464 Patent is directed to "updating a filtering system which controls access to Internet websites/pages." '464 Patent, 1:53-55.

29. Prior to the invention of the '464 Patent, there were "several problems for controlling access to inappropriate information, such as pornography." *Id.*, 1:15-17. To block access to inappropriate sites, databases containing the uniform resource locator ("URL") addresses of websites to be blocked were developed. *Id.*, 1:28-30. Users were then unable to "access any URL found in the database." *Id.*, 1:30-35. However, such databases could never be complete as "new servers and URLs are being added to the Internet on a daily basis." *Id.*, 1:36-41. Thus, such databases could not provide a complete solution. *Id.*

30. The '464 Patent allows for the real-time analysis of URLs that are not found in an existing database of blocked sites in order to update the database and thus, effectively control access to new and/or previously unseen inappropriate websites. *Id.*, 1:45-2:37.

31. The ’464 Patent provides a technical solution to a problem rooted in computer technology and provides an improvement over prior art systems and methods of controlling access to inappropriate and/or harmful websites.

U.S. Patent No. 8,938,773

32. On January 20, 2015, the USPTO issued U.S. Patent No. 8,938,773 (the “’773 Patent”), titled “System and Method for Adding Context to Prevent Data Leakage over a Computer Network.” The ’773 Patent is valid and enforceable. A copy of the ’773 Patent is attached as Exhibit 2.

33. Forcepoint is the owner of all rights, title, and interest in and to the ’773 Patent, and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the ’773 Patent.

34. The ’773 Patent generally relates to computer network security and to systems and methods for preventing data leakage over a computer network. Computer networks are used to transmit data. The invention of the ’773 Patent classifies the data and determines contextual information about the data. Contextual information can be sender contextual information and/or destination contextual information. ’773 Patent, 1:52–53. The network then determines a transmission policy in response to classification and contextual information of the data. The data, based on the classification and contextual information, is either transmitted or blocked.

35. The network of the ’773 Patent includes a classification module for determining the type of data, a context information module for determining the contextual information, a policy/reporting module for generating the transmission policy, and an enforcement module for either transmitting the data, blocking the data, and/or reporting the transmission of the data. *Id.*, 1:64–2:2.

36. The ’773 Patent provides a technical solution to a problem rooted in computer technology and provides an improvement over prior art systems and methods of preventing data leakage over a computer network.

U.S. Patent No. 8,978,140

37. On March 10, 2015, the USPTO issued U.S. Patent No. 8,978,140 (the “’140 Patent”), titled “System and Method of Analyzing Web Content.” The ’140 Patent is valid and enforceable. A copy of the ’140 Patent is attached as Exhibit 3.

38. Forcepoint is the owner of all rights, title, and interest in and to the ’140 Patent, and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the ’140 Patent.

39. The ’140 Patent generally relates to data and application security, specifically to methods of collecting and mining data to determine whether the data includes malicious content. As use of Internet has increased, so has the ability for malicious content to infect networks and those connected to networks over the internet. Newer web applications and content provide significant functionality to websites; however, they also provide opportunities for malicious code to be downloaded to client computers. ’140 Patent, 1:55-60. Hackers write malicious code and applications which utilize vulnerabilities and download themselves onto a computer without relying on activity from the user. *Id.*, 1:65–2:2. For example, malicious code may be embedded into an active content object on a website. That code, if configured to exploit a vulnerability in the web browser, could infect or harm a user. *Id.*, 2:3–5.

40. The invention of the ’140 Patent relates to a system and method to allow for detection of such malicious web content without compromising user functionality. This method and system detects web-based content and quickly identifies and categorizes its behavior,

providing protection from the malicious content to a high volume of client computers with minimal delay. *Id.*, 2:21–27.

41. The '140 Patent provides a technical solution to a problem rooted in computer technology and provides an improvement over prior art systems and methods of collecting and mining data to determine whether the data includes malicious content.

U.S. Patent No. 9,609,001

42. On March 28, 2017, the USPTO issued U.S. Patent No. 9,609,001 (the "'001 Patent"), titled "System and Method for Adding Context to Prevent Data Leakage over a Computer Network." The '001 patent is valid and enforceable. A copy of the '001 Patent is attached as Exhibit 4.

43. Forcepoint is the owner of all rights, title, and interest in and to the '001 Patent, and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '001 Patent.

44. The '001 Patent generally relates to computer network security and to systems and methods for preventing data leakage over a computer network. Computer networks are used to transmit data. The invention of the '001 Patent classifies the data and determines contextual information about the data. Contextual information can be sender contextual information and/or destination contextual information. '001 Patent, 1:59–60. The network then determines a transmission policy in response to classification and contextual information of the data. The data, based on the classification and contextual information, is either transmitted or blocked.

45. The network of the '001 Patent includes a classification module for determining the type of data, a context information module for determining the contextual information, a policy/reporting module for generating the transmission policy, and an enforcement module for

either transmitting the data, blocking the data, and/or reporting the transmission of the data. *Id.*, 2:4–10.

46. The ’001 Patent provides a technical solution to a problem rooted in computer technology and provides an improvement over prior art systems and methods of preventing data leakage over a computer network.

U.S. Patent No. 9,654,495

47. On May 16, 2017, the USPTO issued U.S. Patent No. 9,654,495 (the “’495 Patent”), titled “System and Method of Analyzing Web Addresses.” The ’495 Patent is valid and enforceable. A copy of the ’495 Patent is attached as Exhibit 5.

48. Forcepoint is the owner of all rights, title, and interest in and to the ’495 Patent, and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the ’495 Patent.

49. The ’495 Patent generally relates to data and application security, disclosing systems and methods of collecting and mining data to predict the content or nature of a web site based on its web address. As web sites have developed over time, they have become more sophisticated, including various content, such as active content that is automatically executed upon visiting a website. ’495 Patent, 1:55–2:7. The invention of the ’495 Patent generally relates to systems and methods of classifying web content and controlling access to such web content. *Id.*, 2:24–31.

50. The ’495 Patent provides a technical solution to a problem rooted in computer technology and provides an improvement over prior art data and application security.

COUNTERCLAIM I
(DECLARATION OF NONINFRINGEMENT OF U.S. PATENT NO. 8,726,389)

51. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

52. Forcepoint has not infringed and does not infringe any valid and enforceable claim of the '389 Patent, directly or indirectly, either literally or by application of the doctrine of equivalents. For example, the Counterclaim-Defendants' Accused Products, alone or in combination, do not meet each and every limitation of claim 1 of the '389 Patent because they do not practice "at a base computer, receiving data . . . wherein said data includes information about events initiated . . . when the computer object is created, configured or runs on the first [or second] remote computer, said information including at least . . . an identity of an object or other entity on which the event is being performed."

53. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

54. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '389 Patent.

55. Forcepoint is entitled to a declaratory judgment that Forcepoint does not infringe and has not infringed, either directly or indirectly, any valid and enforceable claim of the '389 Patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM II
(DECLARATION OF INVALIDITY OF U.S. PATENT NO. 8,726,389)

56. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

57. The claims of the ’389 Patent are invalid for failure to meet the conditions of patentability and/or otherwise comply with one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

58. For example, the asserted claims of the ’389 Patent are invalid based on U.S. Patent No. 7,865,956.

59. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

60. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the ’389 Patent.

COUNTERCLAIM III
(DECLARATION OF NONINFRINGEMENT OF U.S. PATENT NO. 10,599,844)

61. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

62. Forcepoint has not infringed and does not infringe any valid and enforceable claim of the ’844 Patent directly or indirectly, either literally or by application of the doctrine of equivalents. For example, the Counterclaim-Defendants’ Accused Products, alone or in combination, do not meet each and every limitation of claim 1 of the ’844 Patent because they do not practice “wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range.”

63. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

64. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '844 Patent.

65. Forcepoint is entitled to a declaratory judgment that Forcepoint does not infringe and has not infringed, either directly or indirectly, any valid and enforceable claim of the '844 Patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM IV
(DECLARATION OF INVALIDITY OF U.S. PATENT NO. 10,599,844)

66. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

67. The claims of the '844 Patent are invalid for failure to meet the conditions of patentability and/or otherwise comply with one or more of §§ 101, 102, 103, and/or 112.

68. For example, the asserted claims of the '844 Patent are invalid based on U.S. Patent No. 9,940,459.

69. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

70. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '844 Patent.

COUNTERCLAIM V
(DECLARATION OF NONINFRINGEMENT OF U.S. PATENT NO. 8,438,386)

71. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

72. Forcepoint has not infringed and does not infringe any valid and enforceable claim of the '386 Patent directly or indirectly, either literally or by application of the doctrine of

equivalents. For example, the Counterclaim-Defendants' Accused Products, alone or in combination, do not meet each and every limitation of claim 1 of the '386 Patent because they do not practice "determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network, the reputation index generated from a reputation vector for the Internet resource, the reputation vector comprising . . . response latency.".

73. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

74. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '386 Patent.

75. Forcepoint is entitled to a declaratory judgment that Forcepoint does not infringe and has not infringed, either directly or indirectly, any valid and enforceable claim of the '386 Patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM VI
(DECLARATION OF INVALIDITY OF U.S. PATENT NO. 8,438,386)

76. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

77. The claims of the '386 Patent are invalid for failure to meet the conditions of patentability and/or otherwise comply with one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

78. For example, the asserted claims of the '386 Patent are invalid based on U.S. Patent No. 8,069,213.

79. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

80. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '386 Patent.

COUNTERCLAIM VII
(DECLARATION OF NONINFRINGEMENT OF U.S. PATENT NO. 9,413,721)

81. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

82. Forcepoint has not infringed and does not infringe any valid and enforceable claim of the '721 Patent directly or indirectly, either literally or by application of the doctrine of equivalents. For example, the Counterclaim-Defendants' Accused Products, alone or in combination, do not meet each and every limitation of claim 1 of the '721 Patent because they do not practice "receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen."

83. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

84. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '721 Patent.

85. Forcepoint is entitled to a declaratory judgment that Forcepoint does not infringe and has not infringed, either directly or indirectly, any valid and enforceable claim of the '721 Patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM VIII
(DECLARATION OF INVALIDITY OF U.S. PATENT NO. 9,413,721)

86. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

87. The claims of the '721 Patent are invalid for failure meet the conditions of patentability and/or otherwise comply with one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

88. For example, the asserted claims of the '721 Patent are invalid based on U.S. Patent No. 8,881,283.

89. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

90. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '721 Patent.

COUNTERCLAIM IX
(DECLARATION OF NONINFRINGEMENT OF U.S. PATENT NO. 10,025,928)

91. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

92. Forcepoint has not infringed and does not infringe any valid and enforceable claim of the '928 Patent directly or indirectly, either literally or by application of the doctrine of equivalents. For example, the Counterclaim-Defendants' Accused Products, alone or in combination, do not meet each and every limitation of claim 1 of the '928 Patent because they do not practice "sending, by the protection agent, the request to one or more web servers" and/or "receiving, at the protection agent on a remote computer, web content from the one or more web

servers, wherein web content comprises data for assembling a web page, and wherein the web content is received in response to the request."

93. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

94. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '928 Patent.

95. Forcepoint is entitled to a declaratory judgment that Forcepoint does not infringe and has not infringed, either directly or indirectly, any valid and enforceable claim of the '928 Patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM X
(DECLARATION OF INVALIDITY OF U.S. PATENT NO. 10,025,928)

96. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

97. The claims of the '928 Patent are invalid for failure to meet the conditions of patentability and/or otherwise comply with one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

98. For example, the asserted claims of the '928 Patent are invalid based on U.S. Patent No. 8,621,613.

99. As a result of the acts described in the foregoing paragraphs, there exists a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.

100. A judicial declaration is necessary and appropriate so that Forcepoint may ascertain its rights regarding the '928 Patent.

COUNTERCLAIM XI
(INFRINGEMENT OF U.S. PATENT NO. 7,194,464)

101. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

102. Counterclaim-Defendants' products and/or services that infringe the '464 Patent include, but are not limited to, the Counterclaim-Defendants' Accused Products and use thereof.

103. Counterclaim-Defendants make, use, sell, offer for sale, and/or import the Counterclaim-Defendants' Accused Products and components thereof in the United States.

104. Counterclaim-Defendants have infringed, either literally or under the doctrine of equivalents, and continue to infringe one or more claims of the '464 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. Forcepoint will continue to suffer irreparable harm unless this Court enjoins Counterclaim-Defendants, their agents, employees, representatives, and all others acting in concert with Counterclaim-Defendants from infringing the '464 Patent.

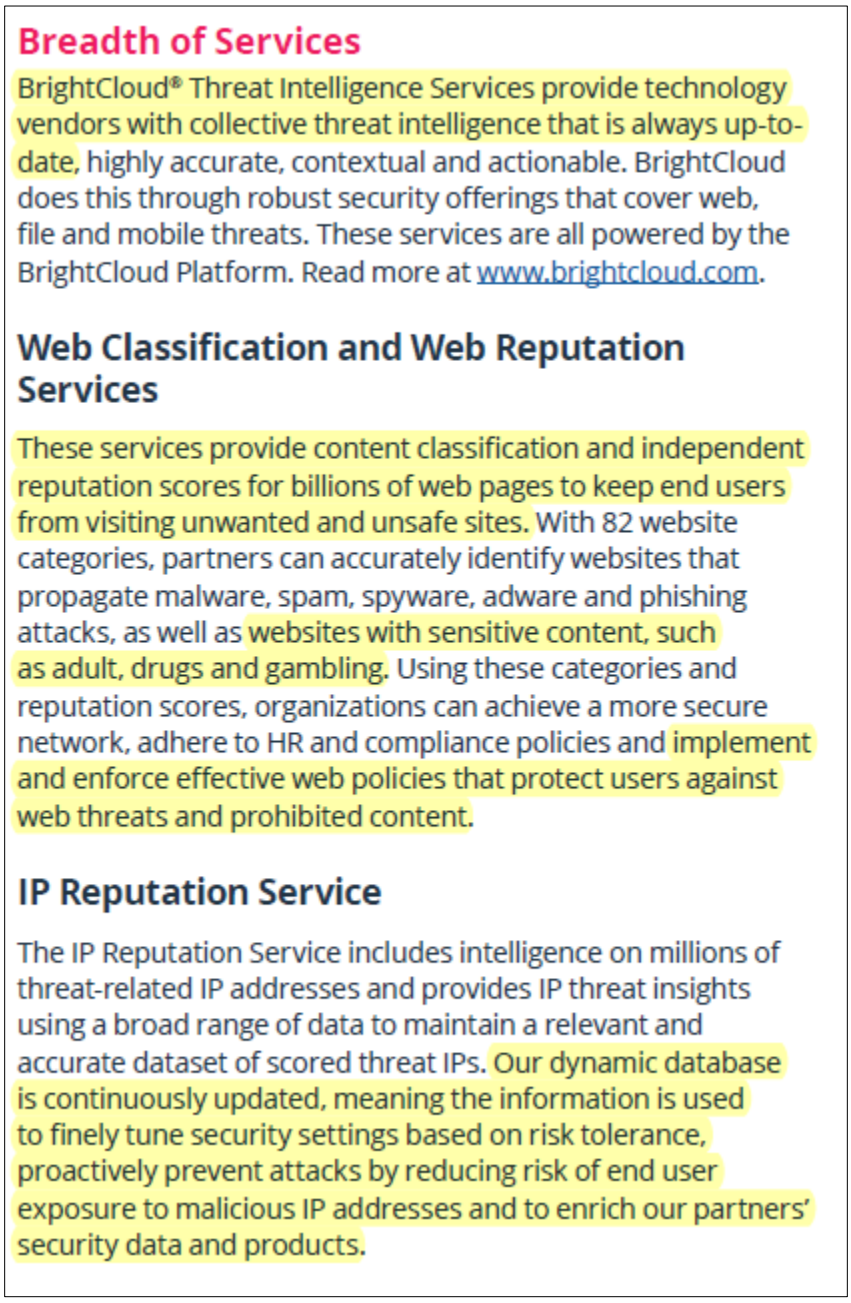
105. Counterclaim-Defendants' Accused Products practice one or more of the '464 Patent's claims. For example, Counterclaim-Defendants' Accused Products, including but not limited to BrightCloud Threat Intelligence Services, practice each element of at least claim 1 of the '464 Patent as demonstrated below.

106. For example, claim 1 of '464 Patent recites:

> A system for collecting identifiers for updating a filtering system which controls access to a wide area network (WAN) of websites/pages, comprising:
>
> a master database including one or more identifiers received from a user to request access to an Internet website/page, and one or more categories associated with each of the one or more identifiers;
>
> an access system coupled to the WAN and configured to send an identifier request if the identifier request is not in the master database; and

a database factory configured to receive the identifier request, select one or more categories to associate with the identifier request if the one or more categories were not previously associated with the identifier, and provide the selected one or more categories to the master database.

107. To the extent the preamble is limiting, Counterclaim-Defendants' Accused Products perform "*[a] system for collecting identifiers for updating a filtering system which controls access to a wide area network (WAN) of websites/pages*." *See, e.g.*:



Breadth of Services

BrightCloud® Threat Intelligence Services provide technology vendors with collective threat intelligence that is always up-to-date, highly accurate, contextual and actionable. BrightCloud does this through robust security offerings that cover web, file and mobile threats. These services are all powered by the BrightCloud Platform. Read more at www.brightcloud.com.

Web Classification and Web Reputation Services

These services provide content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites. With 82 website categories, partners can accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and reputation scores, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

IP Reputation Service

The IP Reputation Service includes intelligence on millions of threat-related IP addresses and provides IP threat insights using a broad range of data to maintain a relevant and accurate dataset of scored threat IPs. Our dynamic database is continuously updated, meaning the information is used to finely tune security settings based on risk tolerance, proactively prevent attacks by reducing risk of end user exposure to malicious IP addresses and to enrich our partners' security data and products.

E.g., Ex. 6 (BrightCloud Threat Intelligence Services DataSheet) at 1.

Real-Time Anti-Phishing Service

The Real-Time Anti-Phishing Service provides effective, live protection against zero-hour phishing attacks, with a focus on low false positives. It determines whether the site poses a phishing risk at the precise moment it is encountered, meaning the analysis and determinations are never stale.

Streaming Malware Detection

Designed to combat polymorphic malware, this innovative technology allows our partners' devices to make determinations at the network level to enable users to quickly allow, block or flag files for investigation.

File Reputation Service

This service provides dynamic file reputation intelligence on known malicious and allowed files to stop malware distribution and enable security teams to focus on actual or potential threats.

E.g., *id.* at 2.

Through the BrightCloud Platform, data is fed into the cloud from millions of global sensors and real-world endpoints, where it is analyzed and correlated with other data points, to provide a comprehensive view of the online threat landscape.

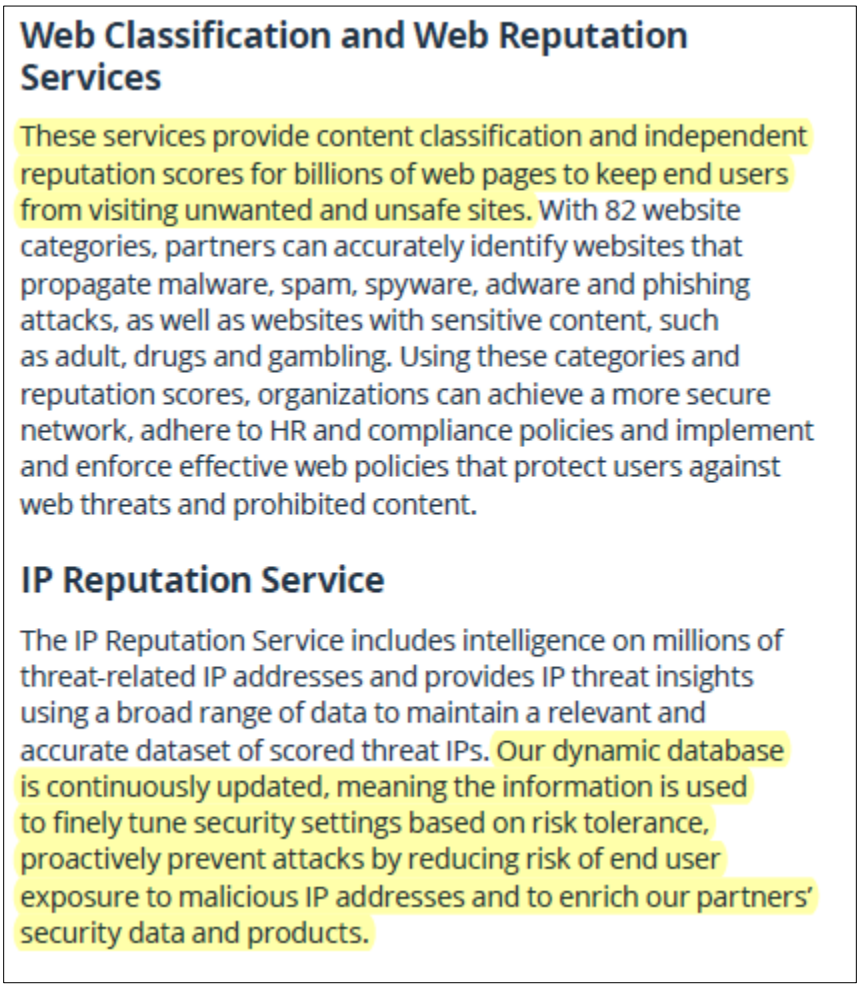
That intelligence is then available to the rest of the network in real-time, including BrightCloud partners through BrightCloud® Threat Intelligence Services. The BrightCloud Platform features limitless scale, lightning-fast data processing and a globally distributed database cluster for high performance and resilience.

Data Correlation for Contextual, Predictive Threat Intelligence

BrightCloud® Threat Intelligence Services use a powerful contextual analysis engine that takes disparate data from BrightCloud Platform feeds and correlates it for deep insight into the landscape of interconnected URLs, IPs, files and mobile apps. Mapping the relationships between these different data points enables BrightCloud to provide partners with highly accurate, up-to-date and actionable intelligence. This also allows BrightCloud to accurately predict how likely an internet object is to be malicious in the future by its associations with other URLs, IPs, files and mobile apps. For example, a seemingly benign IP, which other services may classify as safe, may be tied to other URLs, IPs, files or mobile apps with histories of dangerous behavior. Our advanced analysis provides a predictive reputation score which enables users to proactively protect themselves through self-defined policies based on their risk tolerance. Each of the BrightCloud® Threat Intelligence Services benefits from this correlation engine to proactively protect users against threats that traditional technologies can't detect.

E.g., *id.*

108. The Counterclaim-Defendants' Accused Products include "*a master database including one or more identifiers received from a user to request access to an Internet website/page, and one or more categories associated with each of the one or more identifiers*." *See, e.g.*:



Web Classification and Web Reputation Services

These services provide content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites. With 82 website categories, partners can accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and reputation scores, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

IP Reputation Service

The IP Reputation Service includes intelligence on millions of threat-related IP addresses and provides IP threat insights using a broad range of data to maintain a relevant and accurate dataset of scored threat IPs. Our dynamic database is continuously updated, meaning the information is used to finely tune security settings based on risk tolerance, proactively prevent attacks by reducing risk of end user exposure to malicious IP addresses and to enrich our partners' security data and products.

E.g., *id.* at 1.

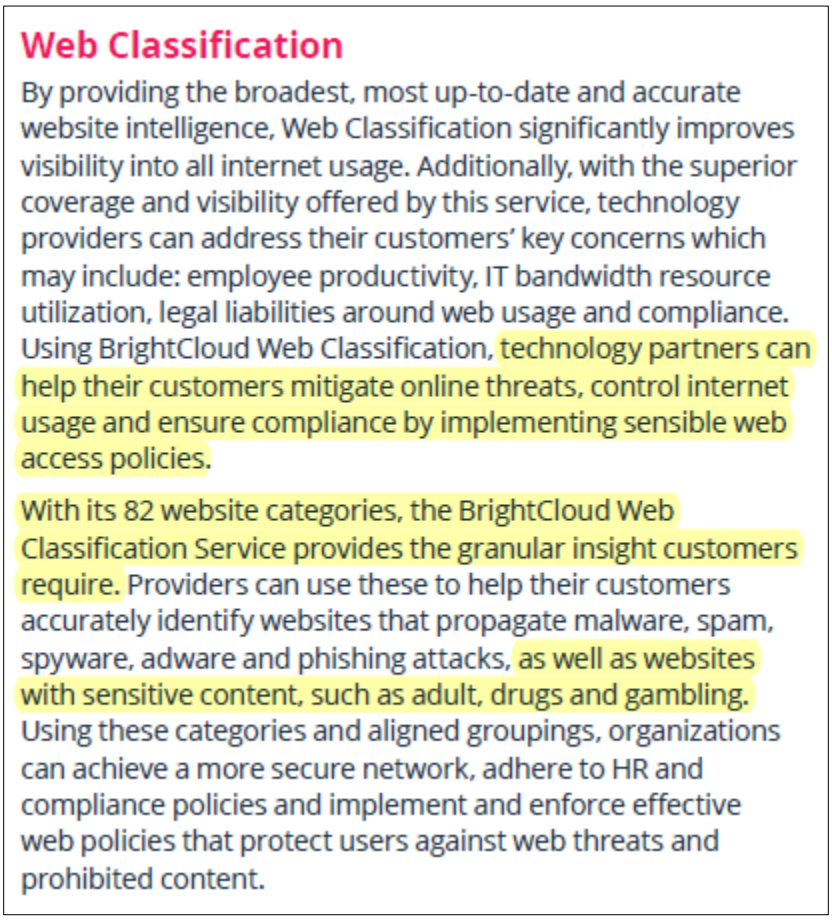
Through the BrightCloud Platform, data is fed into the cloud from millions of global sensors and real-world endpoints, where it is analyzed and correlated with other data points, to provide a comprehensive view of the online threat landscape.

That intelligence is then available to the rest of the network in real-time, including BrightCloud partners through BrightCloud® Threat Intelligence Services. The BrightCloud Platform features limitless scale, lightning-fast data processing and a globally distributed database cluster for high performance and resilience.

Data Correlation for Contextual, Predictive Threat Intelligence

BrightCloud® Threat Intelligence Services use a powerful contextual analysis engine that takes disparate data from BrightCloud Platform feeds and correlates it for deep insight into the landscape of interconnected URLs, IPs, files and mobile apps. Mapping the relationships between these different data points enables BrightCloud to provide partners with highly accurate, up-to-date and actionable intelligence. This also allows BrightCloud to accurately predict how likely an internet object is to be malicious in the future by its associations with other URLs, IPs, files and mobile apps. For example, a seemingly benign IP, which other services may classify as safe, may be tied to other URLs, IPs, files or mobile apps with histories of dangerous behavior. Our advanced analysis provides a predictive reputation score which enables users to proactively protect themselves through self-defined policies based on their risk tolerance. Each of the BrightCloud® Threat Intelligence Services benefits from this correlation engine to proactively protect users against threats that traditional technologies can't detect.

E.g., *id.* at 2.



Web Classification

By providing the broadest, most up-to-date and accurate website intelligence, Web Classification significantly improves visibility into all internet usage. Additionally, with the superior coverage and visibility offered by this service, technology providers can address their customers' key concerns which may include: employee productivity, IT bandwidth resource utilization, legal liabilities around web usage and compliance. Using BrightCloud Web Classification, technology partners can help their customers mitigate online threats, control internet usage and ensure compliance by implementing sensible web access policies.

With its 82 website categories, the BrightCloud Web Classification Service provides the granular insight customers require. Providers can use these to help their customers accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and aligned groupings, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

E.g., Ex. 7 (BrightCloud Web Classification and Web Reputation Services DataSheet) at 1.

Web Reputation

BrightCloud® Web Reputation delivers an up-to-date security check of the websites users visit. This enables technology partners to add a layer of real-time security to their customers' web defenses by accurately assessing the risk posed when opening a URL, independent of its site category.

While the complementary BrightCloud Web Classification Service provides site classification across 82 categories, the Web Reputation Service offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk. The service also provides domain-level reputation scores based on the domain's threat history, age, popularity and other factors, such as its underlying URLs. These reputation tiers enable partners' customers to finely tune their security settings based on their risk tolerance and proactively prevent attacks by limiting the risk of end user exposure to inappropriate or malicious web content.

E.g., *id.* at 2.

Premium Feature: Domain Safety Score

The Domain Safety Score, available as a premium feature within the Web Classification and Web Reputation Services, can help address the issue HTTPS protocols may present, in which categorization at the domain level may not reflect the actual path-level content. Network devices that do not or cannot implement SSL/TLS decryption functionality due to limited resources, cost or capabilities will be enabled to make better security filtering decisions in situations with minimal page-level visibility.

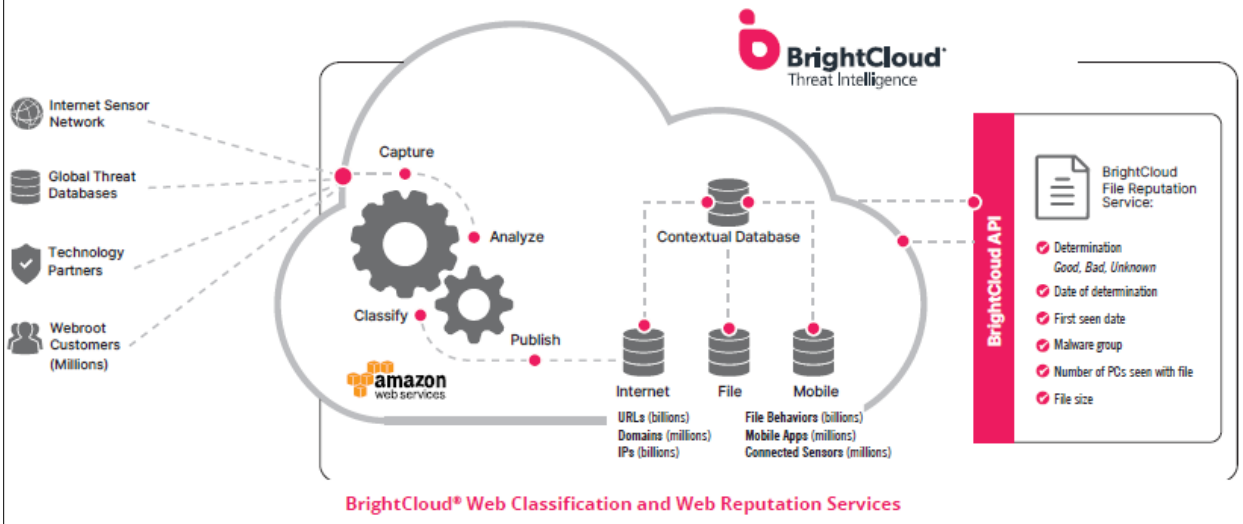
Using the Web Classification and Web Reputation Services, organizations can implement and enforce effective web policies that protect users against web threats and prohibited content, even when encrypted through HTTPS.

BrightCloud Platform

The BrightCloud® Web Classification and Web Reputation Services are powered by the BrightCloud Platform. Data on new and known sites is continuously created and refreshed, ensuring that site categorizations and reputation scores are always as current as possible.

Whenever a user visits an uncategorized site, it is dynamically crawled and scored. Each website's score is checked and adjusted over time.

As part of our ongoing efforts to enhance the BrightCloud Platform, we have introduced new threat hunting techniques, which have enabled more accurate detection and classification of malicious URLs. BrightCloud uses a proprietary and fully automated deep crawling infrastructure for threat hunting, which is combined with the BrightCloud contextual data to scan and accurately categorize thousands of URLs per second. The proactive and methodical parsing of massive quantities of network data enables the BrightCloud Platform to uncover significantly more malware URLs and to determine that, on average, 91% of the new malicious URLs discovered each day are zero-day sites. With its highly sophisticated combination of global threat sensors, machine learning algorithms and human classification, the BrightCloud Platform continuously maintains and expands its knowledge of website classifications and integrates this information for our partners.



BrightCloud® Web Classification and Web Reputation Services

E.g., *id.*

109. The Counterclaim-Defendants' Accused Products include "*an access system coupled to the WAN and configured to send an identifier request if the identifier request is not in the master database*." *See, e.g.*:

Premium Feature: Domain Safety Score

The Domain Safety Score, available as a premium feature within the Web Classification and Web Reputation Services, can help address the issue HTTPS protocols may present, in which categorization at the domain level may not reflect the actual path-level content. Network devices that do not or cannot implement SSL/TLS decryption functionality due to limited resources, cost or capabilities will be enabled to make better security filtering decisions in situations with minimal page-level visibility.

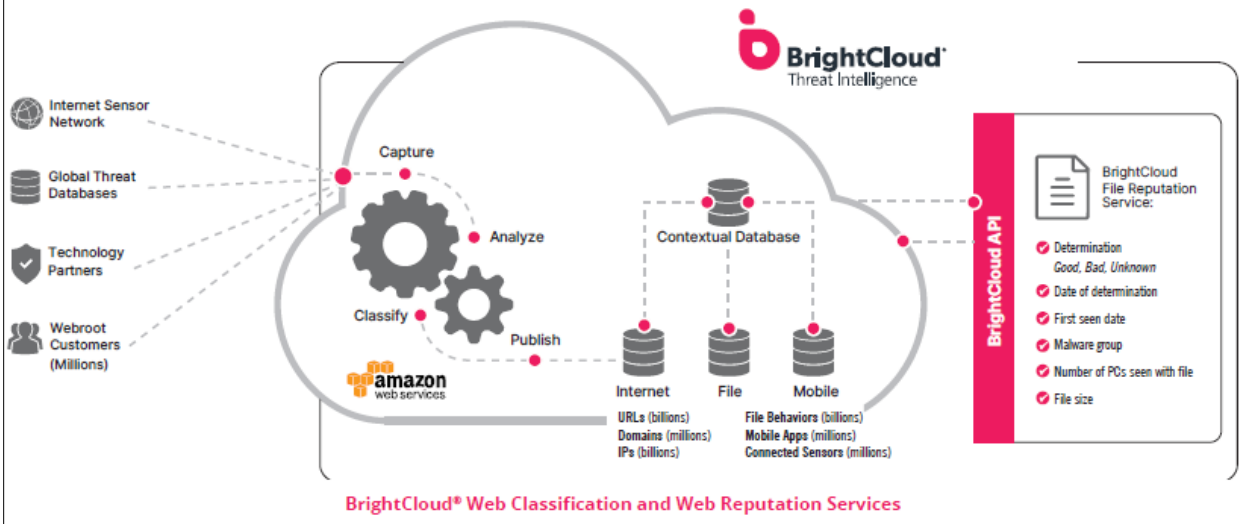
Using the Web Classification and Web Reputation Services, organizations can implement and enforce effective web policies that protect users against web threats and prohibited content, even when encrypted through HTTPS.

BrightCloud Platform

The BrightCloud® Web Classification and Web Reputation Services are powered by the BrightCloud Platform. Data on new and known sites is continuously created and refreshed, ensuring that site categorizations and reputation scores are always as current as possible.

Whenever a user visits an uncategorized site, it is dynamically crawled and scored. Each website's score is checked and adjusted over time.

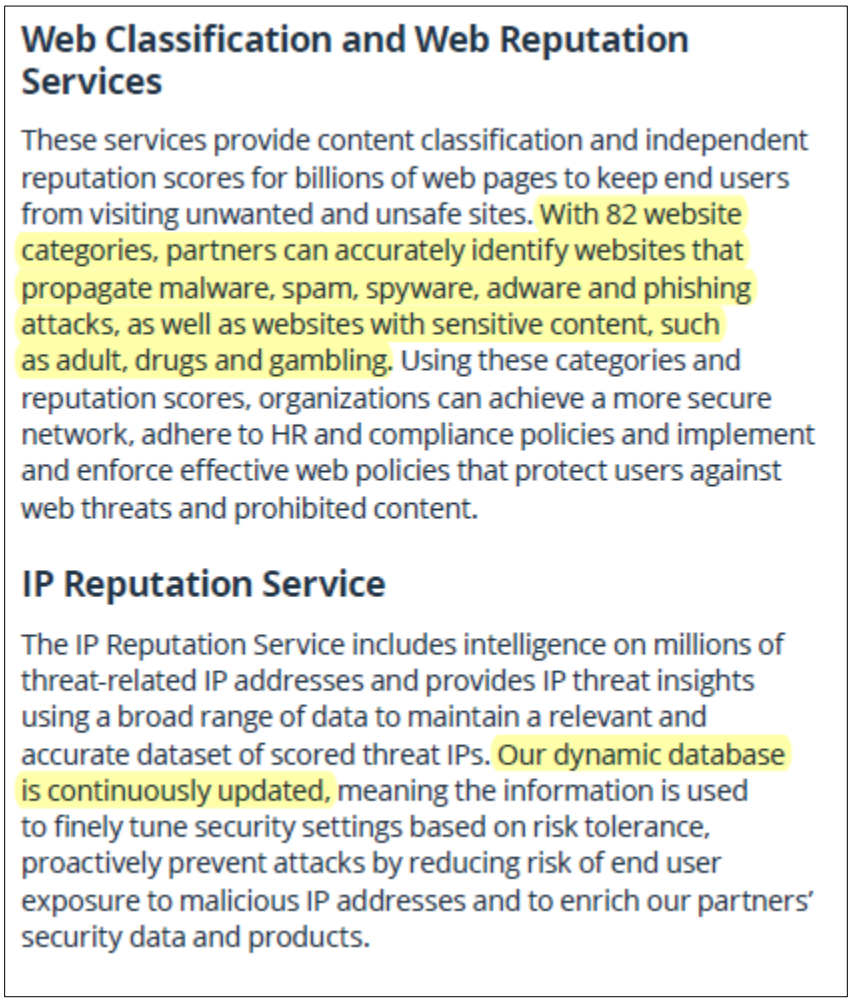
As part of our ongoing efforts to enhance the BrightCloud Platform, we have introduced new threat hunting techniques, which have enabled more accurate detection and classification of malicious URLs. BrightCloud uses a proprietary and fully automated deep crawling infrastructure for threat hunting, which is combined with the BrightCloud contextual data to scan and accurately categorize thousands of URLs per second. The proactive and methodical parsing of massive quantities of network data enables the BrightCloud Platform to uncover significantly more malware URLs and to determine that, on average, 91% of the new malicious URLs discovered each day are zero-day sites. With its highly sophisticated combination of global threat sensors, machine learning algorithms and human classification, the BrightCloud Platform continuously maintains and expands its knowledge of website classifications and integrates this information for our partners.



BrightCloud® Web Classification and Web Reputation Services

E.g., *id.*

110. The Counterclaim-Defendants' Accused Products include "*a database factory configured to receive the identifier request, select one or more categories to associate with the identifier request if the one or more categories were not previously associated with the identifier, and provide the selected one or more categories to the master database*." *See, e.g.*:



Web Classification and Web Reputation Services

These services provide content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites. With 82 website categories, partners can accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and reputation scores, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

IP Reputation Service

The IP Reputation Service includes intelligence on millions of threat-related IP addresses and provides IP threat insights using a broad range of data to maintain a relevant and accurate dataset of scored threat IPs. Our dynamic database is continuously updated, meaning the information is used to finely tune security settings based on risk tolerance, proactively prevent attacks by reducing risk of end user exposure to malicious IP addresses and to enrich our partners' security data and products.

E.g., Ex. 6 at 2.

Premium Feature: Domain Safety Score

The Domain Safety Score, available as a premium feature within the Web Classification and Web Reputation Services, can help address the issue HTTPS protocols may present, in which categorization at the domain level may not reflect the actual path-level content. Network devices that do not or cannot implement SSL/TLS decryption functionality due to limited resources, cost or capabilities will be enabled to make better security filtering decisions in situations with minimal page-level visibility.

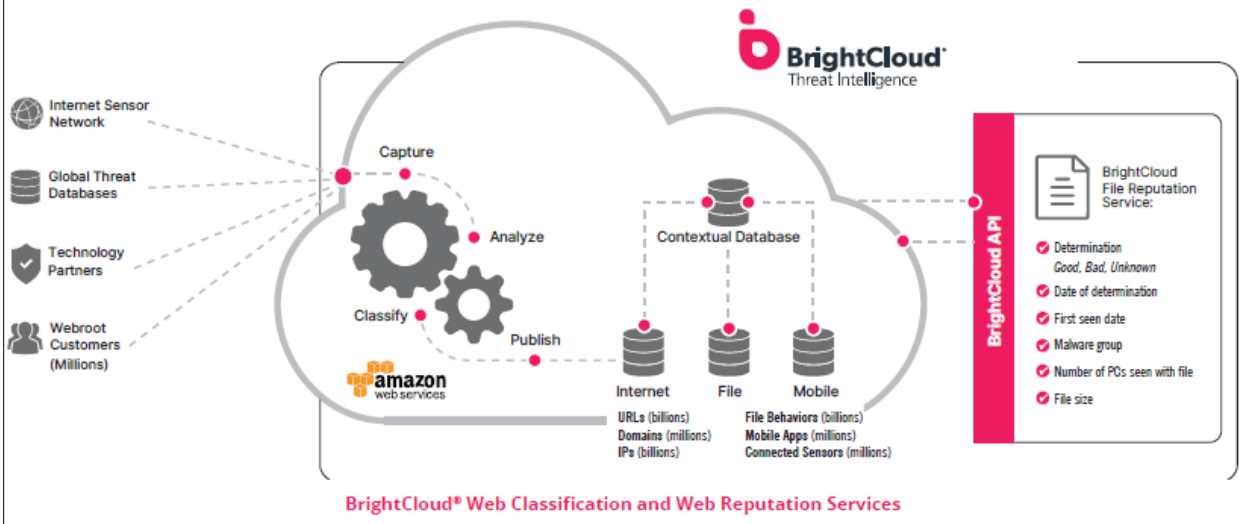
Using the Web Classification and Web Reputation Services, organizations can implement and enforce effective web policies that protect users against web threats and prohibited content, even when encrypted through HTTPS.

BrightCloud Platform

The BrightCloud® Web Classification and Web Reputation Services are powered by the BrightCloud Platform. Data on new and known sites is continuously created and refreshed, ensuring that site categorizations and reputation scores are always as current as possible.

Whenever a user visits an uncategorized site, it is dynamically crawled and scored. Each website's score is checked and adjusted over time.

As part of our ongoing efforts to enhance the BrightCloud Platform, we have introduced new threat hunting techniques, which have enabled more accurate detection and classification of malicious URLs. BrightCloud uses a proprietary and fully automated deep crawling infrastructure for threat hunting, which is combined with the BrightCloud contextual data to scan and accurately categorize thousands of URLs per second. The proactive and methodical parsing of massive quantities of network data enables the BrightCloud Platform to uncover significantly more malware URLs and to determine that, on average, 91% of the new malicious URLs discovered each day are zero-day sites. With its highly sophisticated combination of global threat sensors, machine learning algorithms and human classification, the BrightCloud Platform continuously maintains and expands its knowledge of website classifications and integrates this information for our partners.



BrightCloud® Web Classification and Web Reputation Services

E.g., Ex. 7 at 2.

111. Counterclaim-Defendants became aware of the '464 Patent at least as of the filing of this First Amended Answer and Counterclaims.

112. Counterclaim-Defendants actively induced and are actively inducing infringement of at least claim 1 of the '464 Patent, in violation of 35 U.S.C. § 271(b).

113. Counterclaim-Defendants' partners, customers, and end-users directly infringe at least claim 1 of the '464 Patent, at least by using the Counterclaim-Defendants' Accused Products.

114. Counterclaim-Defendants knowingly induce infringement of at least claim 1 of the '464 Patent by partners, customers, and end-users of the Counterclaim-Defendants' Accused Products with specific intent to induce infringement, and/or with willful blindness to the possibility that its acts induce infringement, through activities relating to the selling, marketing, advertising promotion, support, and distribution of the Counterclaim-Defendants' Accused Products in the United States.

115. Counterclaim-Defendants instruct partners, customers, and end-users, at least through its marketing, promotional, and instructional materials, to use the infringing Counterclaim-Defendants' Accused Products.

116. Counterclaim-Defendants contributed and are contributing to infringement of at least claim 1 of the '464 Patent, in violation of 35 U.S.C. § 271(c) by making, using, offering to sell, selling, and importing the Counterclaim-Defendants' Accused Products and/or components thereof which constitute material parts of the claimed inventions of the '464 Patent and have no substantial non-infringing uses.

117. Counterclaim-Defendants' infringement of the '464 Patent has been knowing and willful since at least the filing of Forcepoint's First Amended Answer and Counterclaims.

118. Counterclaim-Defendants' continued infringement of the '464 Patent has damaged and will continue to damage Forcepoint.

119. Unless and until enjoined by this Court, Counterclaim-Defendants will continue to directly infringe as well as induce and contribute to infringement of the '464 Patent.

Counterclaim-Defendants' infringing acts are causing and will continue to cause at least Forcepoint irreparable harm, for which there is no adequate remedy at law. Under 35 U.S.C. § 283, Forcepoint is entitled to a permanent injunction against further infringement.

COUNTERCLAIM XII
(INFRINGEMENT OF U.S. PATENT NO. 8,938,773)

120. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

121. Counterclaim-Defendants' products and/or services that infringe the '773 Patent include, but are not limited to, the Counterclaim-Defendants' Accused Products and use thereof.

122. Counterclaim-Defendants make, use, sell, offer for sale, and/or import the Counterclaim-Defendants' Accused Products and components thereof in the United States.

123. Counterclaim-Defendants have infringed, either literally or under the doctrine of equivalents, and continue to infringe one or more claims of the '773 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. Forcepoint will continue to suffer irreparable harm unless this Court enjoins Counterclaim-Defendants, their agents, employees, representatives, and all others acting in concert with Counterclaim-Defendants from infringing the '773 Patent.

124. Counterclaim-Defendants' Accused Products practice one or more of the '773 Patent's claims. For example, Counterclaim-Defendants' Accused Products, including but not limited to Webroot DLP and OpenText Documentum, practice each element of at least claim 1 of the '773 Patent as demonstrated below.

125. For example, claim 1 of the '773 Patent recites:

> A system for preventing unauthorized transmission of data over a computer network, the system comprising:

a network gateway device in communication with the computer network, the network gateway device configured to receive data in transit between a source and a destination, wherein the network gateway device comprises:

a classification module configured to determine whether the data in transit includes prohibited content;

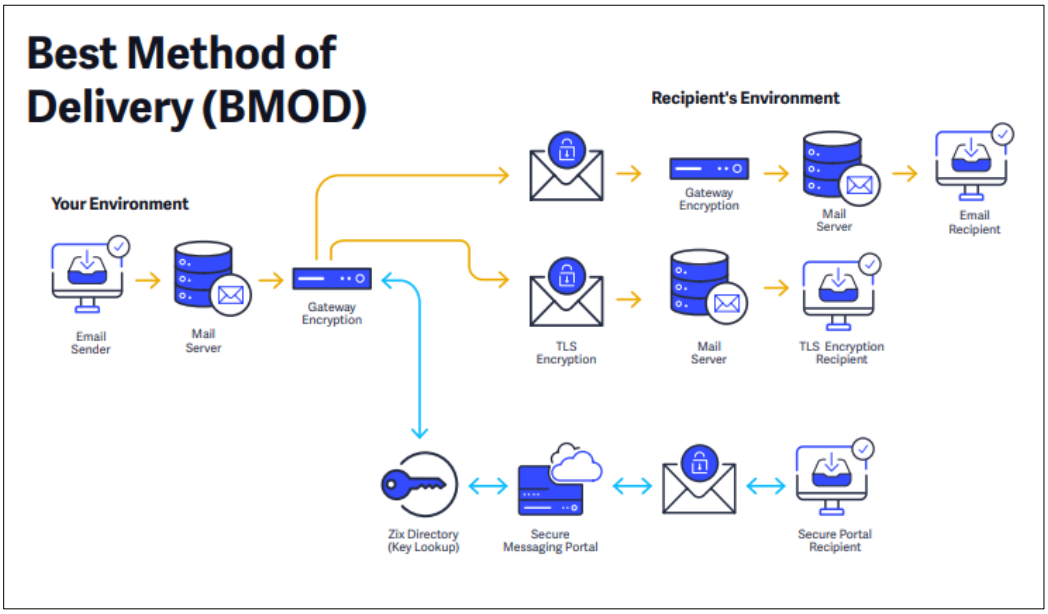
a context information module configured to generate sender contextual information related to the source of the received data and destination contextual information related to the destination of the received data, wherein the destination contextual information comprises a categorization of the Internet Protocol (IP) address of the destination, and wherein the categorization of the IP address of the destination is based at least in part on website content stored at the destination; and

a transmission policy module configured to determine a transmission policy based on the determination of the classification module and the sender contextual information and the destination contextual information.

126. To the extent the preamble is limiting, Counterclaim-Defendants Accused Products perform "*a system for preventing unauthorized transmission of data over a computer network*." For example, Webroot's DLP includes the "ability to . . . proactively defend and protect against email-borne threats . . . . This applies to both inbound and outbound email messages." Ex. 8 (https://www.webroot.com/us/en/business/products/email-security) at 1. OpenText's Documentum "keep[s] content secure and . . . ensur[es] that employees do not access unapproved or superseded information." Ex. 9 (https://www.opentext.com/products-and-solutions/products/enterprise-content-management/documentum-platform) at 3.

127. Counterclaim-Defendants' Accused Products also contain "*a network gateway device in communication with the computer network, the network gateway device configured to receive data in transit between a source and a destination*." For example, Webroot's DLP policies are built into Advanced Email Encryption, such that an "organization can run efficiently while protecting and monitoring sensitive information sent by [] employees." Ex. 10 (https://www-cdn.webroot.com/9816/5409/6025/Carbonite-

Webroot_Protect_Your_Email_Data_Automatically_with_Webroot_Data_Loss_Prevention_Letter_DS_AMER_EN.pdf) at 3.



Ex. 11 (https://zix.com/sites/default/files/2021-10/Zix_Advanced-Email-Encryption_DataSheet_v3.pdf) at 2. OpenText's Documentum includes cloud and on-premises deployment options. Ex. 9 at 9. OpenText's Cloud Managed Services include security and compliance options, including Webroot's Endpoint and Network Security options and Threat Intelligence Services. Ex. 12 (https://www.opentext.com/products-and-solutions/products/opentext-cloud/opentext-security-cloud) at 1.

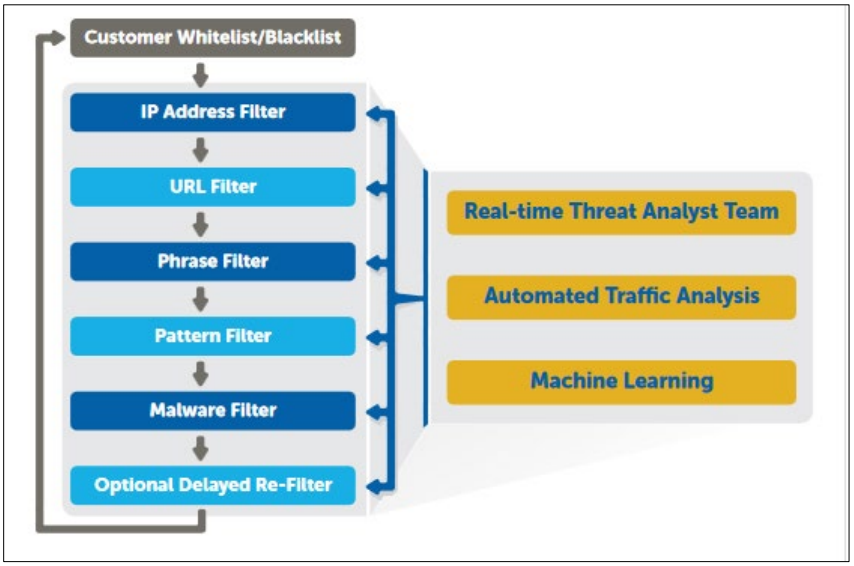
128. Counterclaim-Defendants' Accused Products include "*wherein the network gateway device comprises: a classification module configured to determine whether the data in transit includes prohibited content*." Webroot's DLP "detect[s] information in email subject, body and attachments" and has the ability to "stop inappropriate content." Ex. 10 at 1, 2. OpenText's Documentum "seamlessly integrate[s] with existing enterprise security and identi[fies] management infrastructure, while automating security based on content attributes and

user roles." Ex. 13 (https://www.opentext.com/products-and-solutions/products/enterprise-content-management/documentum-platform/documentum-governance-compliance) at 4.

129. Counterclaim-Defendants' Accused Products include "*a context information module configured to generate sender contextual information related to the source of the received data and destination contextual information related to the destination of the received data*." For example, Webroot's DLP includes user management features (Ex. 11 at 2) and "stop[s] messages sent by unauthorized users and hold[s] for review . . . . For example, a bank teller sending financial data externally or an intern sending customer data to a personal account." Ex. 10 at 2. Likewise, OpenText's Documentum D2 "offers a configuration tool and rules engine that governs the policies and behaviors of content in OpenText Documentum." Ex. 15 (https://www.opentext.com/products-and-solutions/products/enterprise-content-management/documentum-platform/documentum-d2) at 2. For example, "OpenText Documentum Information Rights Management Services controls, secures and tracks sensitive information wherever it resides—within a workgroup, across departments and agencies or with partners and suppliers outside the firewall." Ex. 16 (https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-po-documentum-records-manager-en.pdf) at 3. Additionally, Documentum provides "access to content and streamline[d] information management with personalized role-based experiences." Ex. 9 at 8. Documentum also "seamlessly integrate[s] with existing enterprise security and identif[ies] management infrastructure while automating security based on content attributes and user roles." Ex. 13 at 4.

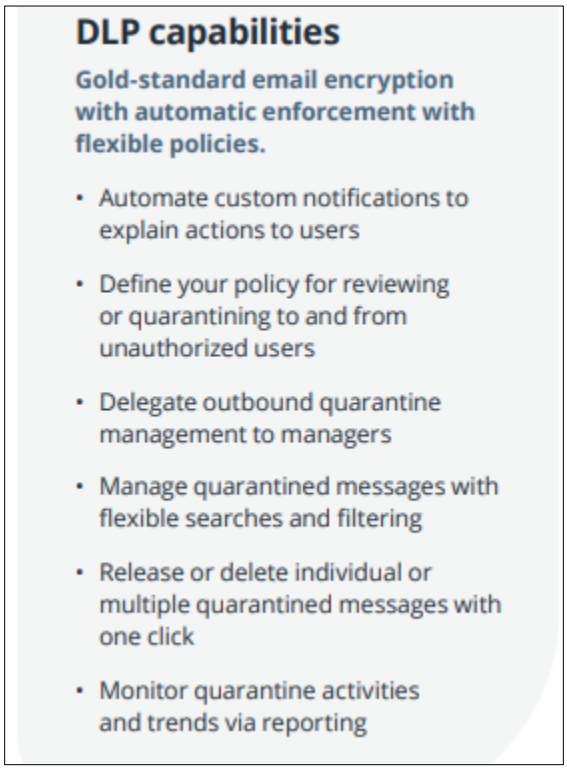
130. Counterclaim-Defendants' Accused Products include "*wherein the destination contextual information comprises a categorization of the Internet Protocol (IP) address of the*

destination, and wherein the categorization of the IP address of the destination is based at least in part on website content stored at the destination." For example, Webroot's DLP also permits various customizations for its security policies, including "blocking or whitelisting of individual URLs or IP addresses." Ex. 17 (https://www.techdata.ca/webroot/files/WEBROOT_Whitepaper%20SaaS%20Biz%20Case%20PRINTa.pdf) at 6. Likewise, Webroot's DLP, which runs on a single console with Zix DLP, includes a "multi-layer filtering engine . . . [and] combines standard IP address and URL filters." Ex. 18 (https://www.securemailencryption.com/ZixProtect-Essentials.asp) at 2.



Id. As another example, OpenText's Documentum "provides client sessions with connection information, such as IP addresses and port numbers." Ex. 19 (https://documentumsite.files.wordpress.com/2016/05/cs_7-1_admin_guide.pdf) at 34. Additionally, "[n]etwork locations identify locations on a network, and optionally, a range of IP addresses, from which users connect to Documentum web clients." Ex. 20 (https://dcc.pttep.com/da/help/en/default.htm?startat=help_da_netloc_config.htm).

131. Counterclaim-Defendants' Accused Products also include "*a transmission policy module configured to determine a transmission policy based on the determination of the classification module and the sender contextual information and the destination contextual information*." For example, Webroot's DLP includes a number of transmission policies with "automatic enforcement." Ex. 10 at 1.



Id. In addition to those policies included in the image above, Webroot DLP also includes transmission policies to "stop messages sent by unauthorized users and hold for review . . . . For example, a bank teller sending financial data externally or an intern sending customer data to a personal account." *Id.* at 2. As another example, OpenText's Documentum includes a "robust, fault-tolerant, cloud-ready architecture to manage and control all information content . . . [and which] scales to meet the most strenuous requirements while ensuring constant governance policies, regardless of location." Ex. 9 at 5. Additionally, OpenText's Documentum D2 "offers

a configuration tool and rules engine that governs the policies and behaviors of content in OpenText Documentum as well as the interaction between content and users." Ex. 15 at 2.

132. Counterclaim-Defendants became aware of the '773 Patent at least as of the filing of Forcepoint's First Amended Answer and Counterclaims.

133. Counterclaim-Defendants actively induced and are actively inducing infringement of at least claim 1 of the '773 Patent, in violation of 35 U.S.C. § 271(b).

134. Counterclaim-Defendants partners, customers, and end-users directly infringe at least claim 1 of the '773 Patent, at least by using the Counterclaim-Defendants' Accused Products.

135. Counterclaim-Defendants knowingly induce infringement of at least claim 1 of the '773 Patent by partners, customers, and end-users of the Counterclaim-Defendants' Accused Products with specific intent to induce infringement, and/or with willful blindness to the possibility that its acts induce infringement, through activities relating to the selling, marketing, advertising promotion, support, and distribution of the Counterclaim-Defendants' Accused Products in the United States.

136. Counterclaim-Defendants instruct partners, customers, and end-users, at least through its marketing, promotional, and instructional materials, to use the infringing Counterclaim-Defendants' Accused Products.

137. Counterclaim-Defendants contributed and are contributing to infringement of at least claim 1 of the '773 Patent, in violation of 35 U.S.C. § 27199(c) by making, using, offering to sell, selling, and importing the Counterclaim-Defendants' Accused Products and/or components thereof which constitute material parts of the claimed inventions of the '773 Patent and have no substantial non-infringing uses.

138. Counterclaim-Defendants' infringement of the '773 Patent has been knowing and willful since at least the filing of Forcepoint's First Amended Answer and Counterclaims.

139. Counterclaim-Defendants' continued infringement of the '773 Patent has damaged and will continue to damage Forcepoint.

140. Unless and until enjoined by this Court, Counterclaim-Defendants will continue to directly infringe as well as induce and contribute to infringement of the '773 Patent. Counterclaim-Defendants' infringing acts are causing and will continue to cause at least Forcepoint irreparable harm, for which there is no adequate remedy at law. Under 35 U.S.C. § 283, Forcepoint is entitled to a permanent injunction against further infringement.

COUNTERCLAIM XIII
(INFRINGEMENT OF U.S. PATENT NO. 8,978,140)

141. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

142. Counterclaim-Defendants' products and/or services that infringe the '140 Patent include, but are not limited to, the Counterclaim-Defendants' Accused Products and use thereof.

143. Counterclaim-Defendants make, use, sell, offer for sale, and/or import the Counterclaim-Defendants' Accused Products and components thereof in the United States.

144. Counterclaim-Defendants have infringed, either literally or under the doctrine of equivalents, and continue to infringe one or more claims of the '140 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. Forcepoint will continue to suffer irreparable harm unless this Court enjoins Counterclaim-Defendants, their agents, employees, representatives, and all others acting in concert with Counterclaim-Defendants from infringing the '140 Patent.

145. Counter-claim Defendants' Accused Products practice one or more of the '140 Patent's claims. For example, Counterclaim-Defendants' Accused Products, including but not limited to BrightCloud Threat Intelligence Services, practice each element of at least claim 1 of the '140 Patent as demonstrated below.

146. For example, claim 1 of the '140 Patent recites:

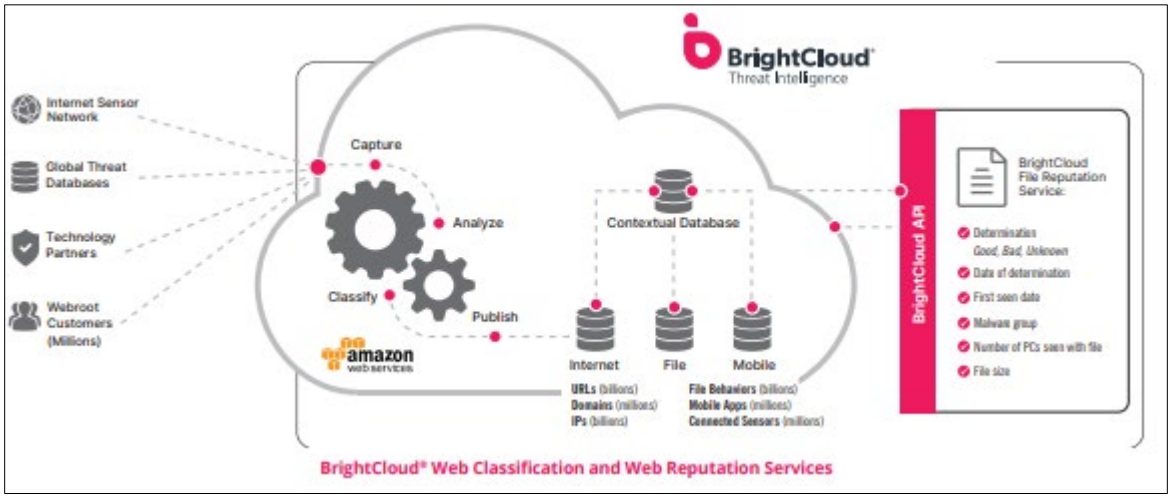
> A computer-implemented method of categorizing a uniform resource locator (URL) based on web content associated with the URL, the method comprising:
>
> identifying a first URL using a first collection method of a plurality of collection methods, wherein each of the plurality of collection methods is performed using at least one electronic processor;
>
> determining, using an electronic processor, whether the first URL contains a malicious data element;
>
> categorizing, using an electronic processor, the first URL in response to a determination that the first URL contains a malicious data element;
>
> in response to determining the first URL does not contain a malicious data element:
>
> assigning, using an electronic processor, a first categorization priority to the first URL based on the first URL being identified using the first collection method, and
>
> categorizing, using an electronic processor, the first URL based on the first categorization priority, wherein categorization of a URL comprises assigning a category to the URL based on a classification of at least one of web content or an Internet Protocol (IP) address identified by the URL;
>
> identifying a second URL using a second collection method, wherein the first collection method and the second collection method are different and each are one of a web crawler, a Domain Name Server (DNS) database, and a honey client;
>
> determining, using an electronic processor, whether the second URL contains a malicious data element;
>
> categorizing, using an electronic processor, the second URL in response to a determination that the second URL contains a malicious data element;
>
> in response to determining the second URL does not contain a malicious data element:

> assigning, using an electronic processor, a second categorization priority different than the first categorization priority based on the second URL having been identified using the second collection method, and
>
> categorizing, using an electronic processor, the second URL based on the second categorization priority.

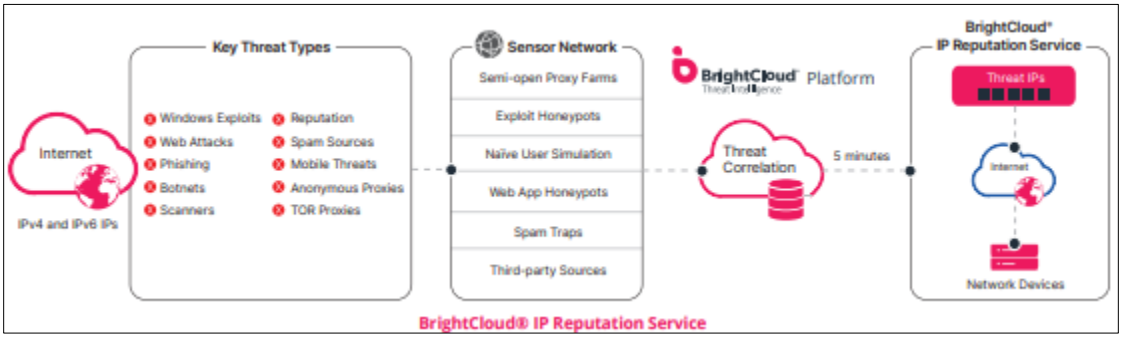
147. To the extent the preamble is limiting, Counterclaim-Defendants' Accused Products perform "*[a] computer-implemented method of categorizing a uniform resource locator (URL) based on web content associated with the URL.*" For example, BrightCloud Threat Intelligence Services "provide content classification and independent reputation scores for billions of web pages . . . ." Ex. 6 at 1. BrightCloud Web Classification and Web Reputation Services, categorizes websites into "82 website categories" so partners can "identify websites that propagate malware, spam, spyware, adware and phishing attacks . . . ." *Id.* BrightCloud IP Reputation Service, "includes intelligence on millions of threat-related IP addresses and provides IP threat insights . . . to maintain a relevant and accurate dataset of scored threat IPs." *Id.* That database of websites is "dynamic" and "continually updated." Real-Time Anti-Phishing service determines whether a website "poses a phishing risk at the precise moment it is encountered . . . ." *Id.* at 2. BrightCloud Threat Intelligence Services also uses a "contextual analysis engine that takes disparate data from BrightCloud Platform feeds and correlates it for deep insight into the landscape of interconnected URLs . . . ." *Id.* It then maps "the relationships between these different data points" which "allows BrightCloud to accurately predict how likely an internet object is to be malicious in the future by its associations with other URLs . . . ." *Id.*

148. Counterclaim-Defendants' Accused Products also include "*identifying a first URL using a first collection method of a plurality of collection methods, wherein each of the plurality of collection methods is performed using at least one electronic processor.*" For example, BrightCloud Web Classification and Web Reputation Services "categorizes the largest URL

database of its kind across 82 categories and scores website and domain risk, regardless of internet category." Ex. 7 at 1. As shown in the diagram below it does this by capturing, analyzing, classifying, and publishing websites found through an "Internet Sensor network."



Id. at 2. The "Sensor Network" includes "Semi-open Proxy Farms," "Exploit Honeypots," "Naïve User Simulation," "Web App Honeypots," "Spam Traps," and "Third-Party Sources" as shown in the diagram below.



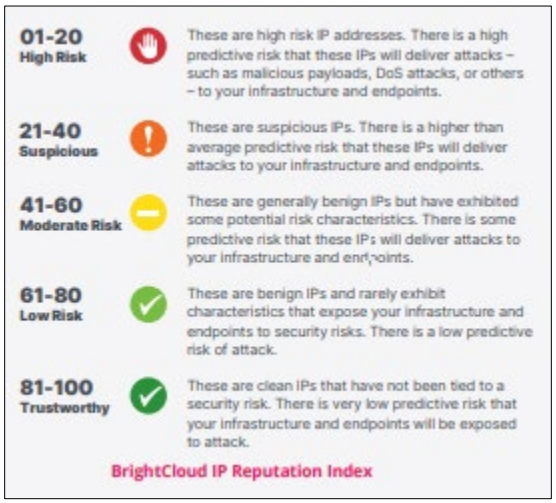
Ex. 21 (https://www-cdn.webroot.com/9716/4556/6849/BrightCloud_IP_Reputation_Service_DS_AMER_EN.pdf) at 2.

149. Counterclaim-Defendants' Accused Products also include "*determining, using an electronic processor, whether the first URL contains a malicious data element*." For example,

BrightCloud Web Classification categorizes websites into "82 categories." These categories "accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with sensitive content . . . ." Ex. 7 at 1. BrightCloud's Web Reputation "offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI)." *Id.* at 2. WRI ranges "from 1 to 100" and classifies URLs into the following tiers: "Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk." *Id.* To categorize, a website into "Trustworthy, Low Risk, Moderate Risk, Suspicious, [or] High Risk" Webroot® WRI must necessarily determine, using an electronic processor, whether the second URL contains a malicious data element.

150. Counterclaim-Defendants' Accused Products also include "*categorizing, using an electronic processor, the first URL in response to a determination that the first URL contains a malicious data element*." For example, "[t]he BrightCloud Web Classification and Web Reputation Services categorizes the largest URL database of its kind across 82 categories and scores website and domain risk, regardless of internet category." *Id.* at 1. This can help customers "accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content . . . ." *Id.* Counterclaim-Defendants advertise that Web Classification allows customers to "achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content." *Id.* To date, BrightCloud has "43+ billion URLs classified" and "6 million dangerous IPs correlated with URLs." *Id.* at 2. BrightCloud's Web Reputation "offers an additional lens through which a site can be evaluated as a potential threat.

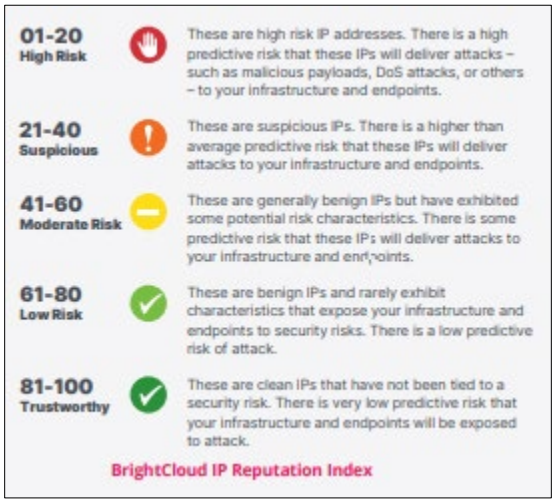
In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI)." *Id.* WRI ranges "from 1 to 100" and classifies URLs into the following tiers: "Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk." *Id.* These categories can be seen in the diagram below.



Ex. 21 at 1.

151. Counterclaim-Defendants' Accused Products also include "*in response to determining the first URL does not contain a malicious data element: assigning, using an electronic processor, a first categorization priority to the first URL based on the first URL being identified using the first collection method*." For example, BrightCloud Web Classification categorizes websites into "82 categories." Ex. 7 at 1. These categories "accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with sensitive content . . . ." *Id.* BrightCloud® Web Reputation "delivers an up-to-date security check of the websites users visits . . . . In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with

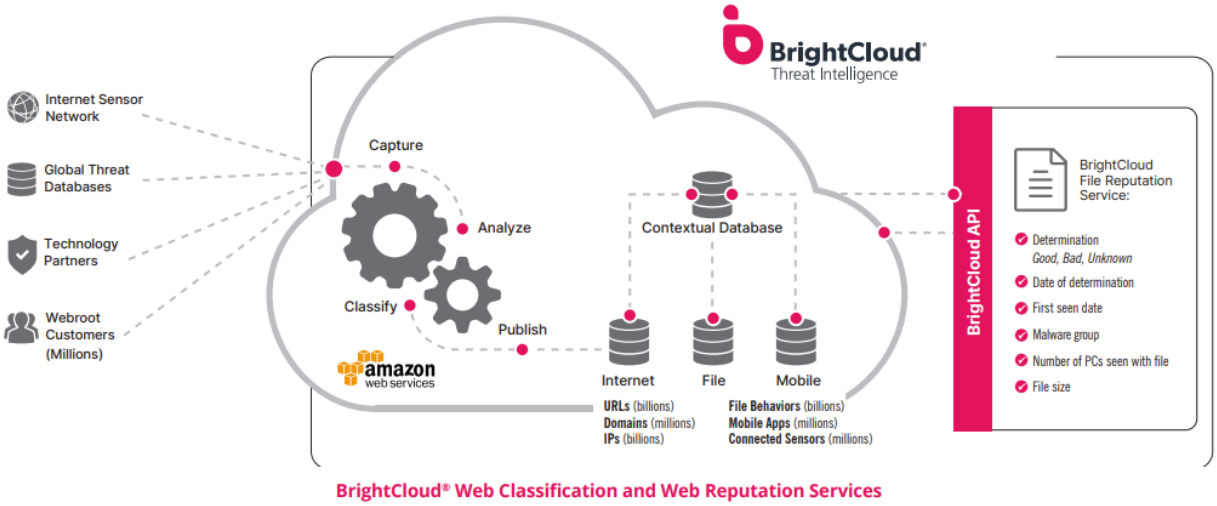
tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk." *Id.* at 2. And illustration of these categorization priorities is shown below:



Ex. 21 at 1.

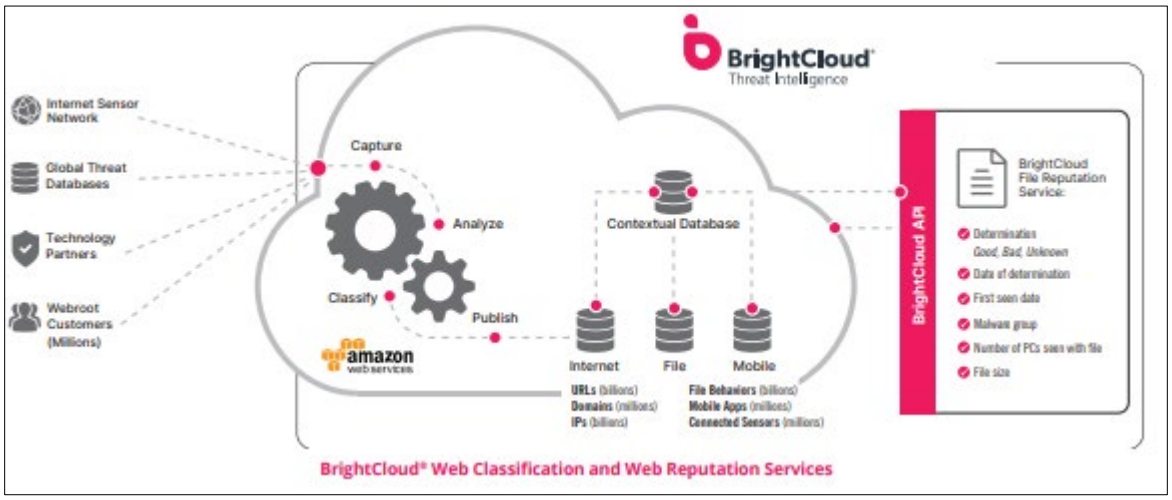
152. Counterclaim-Defendants' Accused Products also include "*categorizing, using an electronic processor, the first URL based on the first categorization priority, wherein categorization of a URL comprises assigning a category to the URL based on a classification of at least one of web content or an Internet Protocol (IP) address identified by the URL*." For example, BrightCloud® Web Reputation "delivers an up-to-date security check of the websites users visits . . . . In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk." Ex. 7 at 2. BrightCloud® Web Classification assigns one of 82 categories to URLs to "help [its] customers accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks as well as websites with sensitive content . . . ." *Id.* at 1. BrightCloud® Web Classification and Web Reputation Services use "cloud-based analytics" and "machine learning" to classify websites. As

shown in the figure below, BrightCloud® Web Classification and Web Reputation Services capture a URL, analyze that URL, classify that URL and then publish that URL to the contextual database.

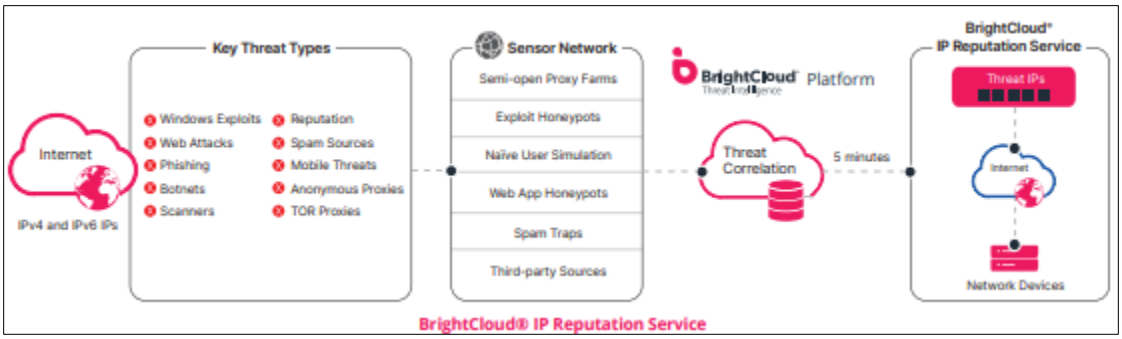


Id. at 2.

153. Counterclaim-Defendants' Accused Products also include "*identifying a second URL using a second collection method, wherein the first collection method and the second collection method are different and each are one of a web crawler, a Domain Name Server (DNS) database, and a honey client*." For example, BrightCloud Web Classification and Web Reputation Services "categorizes the largest URL database of its kind across 82 categories and scores website and domain risk, regardless of internet category." *Id.* at 1. As shown in the diagram below it does this by capturing, analyzing, classifying, and publishing websites found through an "Internet Sensor network."



Id. at 2. The "Sensor Network" includes multiple methods of capturing a URL, including "Semi-open Proxy Farms," "Exploit Honeypots," "Naïve User Simulation," "Web App Honeypots," "Spam Traps," and "Third-Party Sources" as shown in the diagram below.

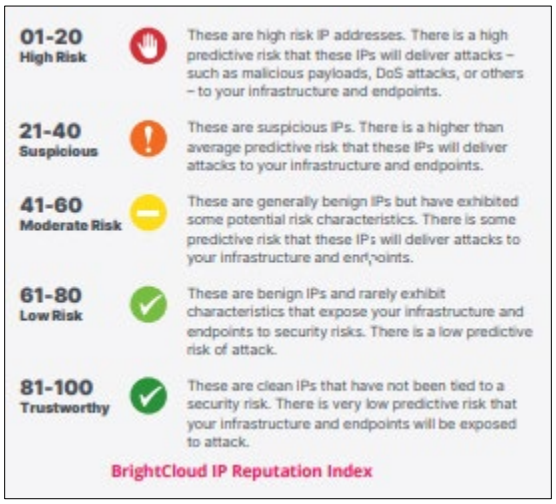


Ex. 21 at 2.

154. Counterclaim-Defendants' Accused Products also include "*determining, using an electronic processor, whether the second URL contains a malicious data element*." For example, BrightCloud Web Classification categorizes websites into "82 categories." These categories "accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with sensitive content . . . ." Ex. 7 at 1. BrightCloud's Web Reputation "offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time

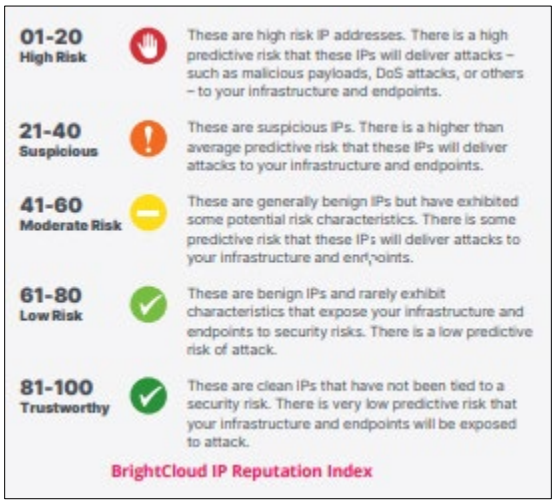
performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI)." *Id.* at 2. WRI ranges "from 1 to 100" and classifies URLs into the following tiers: "Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk." *Id.* To categorize, a website into "Trustworthy, Low Risk, Moderate Risk, Suspicious, [or] High Risk" Webroot® WRI must necessarily determine, using an electronic processor, whether the second URL contains a malicious data element.

155. Counterclaim-Defendants' Accused Products also include *"categorizing, using an electronic processor, the second URL in response to a determination that the second URL contains a malicious data element*." For example, "[t]he BrightCloud Web Classification and Web Reputation Services categorizes the largest URL database of its kind across 82 categories and scores website and domain risk, regardless of internet category." *Id.* at 1. This can help customers "accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content . . . ." *Id.* Counterclaim-Defendants advertise that Web Classification allows customers to "achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content." *Id.* To date, BrightCloud has "43+ billion URLs classified" and "6 million dangerous IPs correlated with URLs." *Id.* at 2. BrightCloud's Web Reputation "offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI)." *Id.* WRI ranges "from 1 to 100" and classifies URLs into the following tiers: "Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk." *Id.* These categories can be seen in the diagram below.



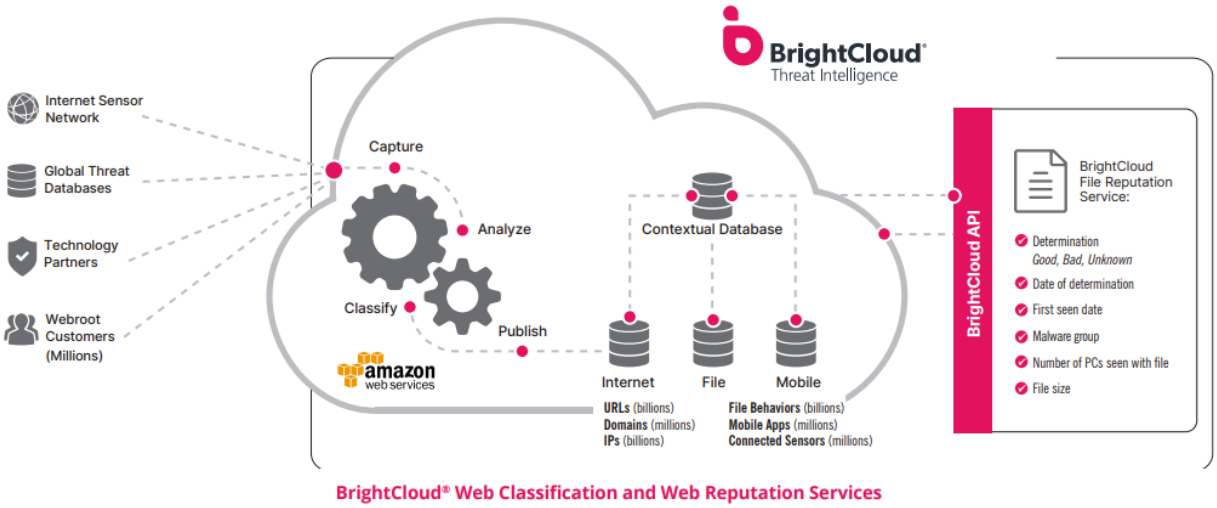
Ex. 21 at 1.

156. Counterclaim-Defendants' Accused Products also include "*in response to determining the second URL does not contain a malicious data element: assigning, using an electronic processor, a second categorization priority different than the first categorization priority based on the second URL having been identified using the second collection method*." For example, BrightCloud Web Classification categorizes websites into "82 categories." These categories "accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with sensitive content . . . ." Ex. 7 at 1. BrightCloud® Web Reputation "delivers an up-to-date security check of the websites users visits . . . . In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk." *Id.* at 2. And illustration of these categorization priorities is shown below:



Ex. 21 at 1.

157. Counterclaim-Defendants' Accused Products also include "*categorizing, using an electronic processor, the second URL based on the second categorization priority*." For example, BrightCloud® Web Reputation "delivers an up-to-date security check of the websites users visits . . . . In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk." Ex. 7 at 2. BrightCloud® Web Classification assigns one of 82 categories to URLs to "help [its] customers accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks as well as websites with sensitive content . . . ." *Id.* at 1. BrightCloud® Web Classification and Web Reputation Services use "cloud-based analytics" and "machine learning" to classify websites. As shown in the figure below, BrightCloud® Web Classification and Web Reputation Services capture a URL, analyze that URL, classify that URL and then publish that URL to the contextual database.



Ex. 7 at 2.

158. Counterclaim-Defendants became aware of the ’140 Patent at least as of the filing of Forcepoint’s First Amended Answer and Counterclaims.

159. Counterclaim-Defendants actively induced and are actively inducing infringement of at least claim 1 of the ’140 Patent, in violation of 35 U.S.C. § 271(b).

160. Counterclaim-Defendants’ partners, customers, and end-users directly infringe at least claim 1 of the ’140 Patent, at least by using the Counterclaim-Defendants’ Accused Products.

161. Counterclaim-Defendants knowingly induce infringement of at least claim 1 of the ’140 Patent by partners, customers, and end-users of the Counterclaim-Defendants’ Accused Products with specific intent to induce infringement, and/or with willful blindness to the possibility that its acts induce infringement, through activities relating to the selling, marketing, advertising promotion, support, and distribution of the Counterclaim-Defendants’ Accused Products in the United States.

162. Counterclaim-Defendants instruct partners, customers, and end-users, at least through its marketing, promotional, and instructional materials, to use the infringing Counterclaim-Defendants' Accused Products.

163. Counterclaim-Defendants contributed and are contributing to infringement of at least claim 1 of the '140 Patent, in violation of 35 U.S.C. § 271(c) by making, using, offering to sell, selling, and importing the Counterclaim-Defendants' Accused Products and/or components thereof which constitute material parts of the claimed inventions of the '140 Patent and have no substantial non-infringing uses.

164. Counterclaim-Defendants' infringement of the '140 Patent has been knowing and willful since at least the filing of Forcepoint's First Amended Answer and Counterclaims.

165. Counterclaim-Defendants' continued infringement of the '140 Patent has damaged and will continue to damage Forcepoint.

166. Unless and until enjoined by this Court, Counterclaim-Defendants will continue to directly infringe as well as induce and contribute to infringement of the '140 Patent. Counterclaim-Defendants' infringing acts are causing and will continue to cause at least Forcepoint irreparable harm, for which there is no adequate remedy at law. Under 35 U.S.C. § 283, Forcepoint is entitled to a permanent injunction against further infringement.

COUNTERCLAIM XIV
(INFRINGEMENT OF U.S. PATENT NO. 9,609,001)

167. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

168. Counterclaim-Defendants' products and/or services that infringe the '001 Patent include, but are not limited to, the Counterclaim-Defendants' Accused Products and use thereof.

169. Counterclaim-Defendants make, use, sell, offer for sale, and/or import the Counterclaim-Defendants' Accused Products and components thereof in the United States.

170. Counterclaim-Defendants have infringed, either literally or under the doctrine of equivalents, and continue to infringe one or more claims of the '001 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. Forcepoint will continue to suffer irreparable harm unless this Court enjoins Counterclaim-Defendants, their agents, employees, representatives, and all others acting in concert with Counterclaim-Defendants from infringing the '001 Patent.

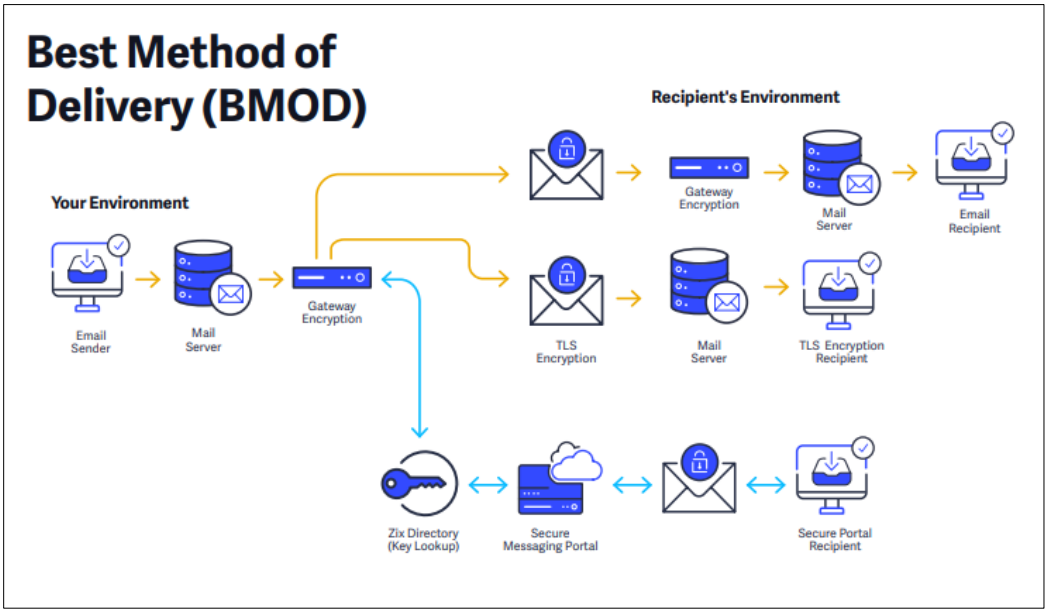
171. Counterclaim-Defendants' Accused Products practice one or more of the '001 Patent's claims. For example, Counterclaim-Defendants' Accused Products, including but not limited to Webroot DLP and OpenText Documentum, practice each element of at least claim 1 of the '001 Patent as demonstrated below.

172. For example, claim 1 of the '001 Patent recites:

> A system for preventing unauthorized transmission of data over a computer network, the system comprising:
>
> a network gateway device in communication with the computer network, the network gateway device configured to receive data in transit between a source and a destination, wherein the network gateway device comprises:
>
> a classification module configured to determine whether the data in transit includes prohibited content;
>
> a context information module configured to generate destination contextual information related to the destination of the received data, wherein the destination contextual information comprises a categorization of an Internet Protocol (IP) address of the destination, and wherein the categorization of the IP address of the destination is based at least in part on website content stored at the destination; and
>
> a transmission policy module configured to determine a transmission policy based on the determination of the classification module and the destination contextual information.

173. To the extent the preamble is limiting, Counterclaim-Defendants' Accused Products perform "*a system for preventing unauthorized transmission of data over a computer network*." For example, Webroot's DLP includes the "ability to . . . proactively defend and protect against email-borne threats . . . . This applies to both inbound and outbound email messages." Ex. 8 at 1. OpenText's Documentum "keep[s] content secure and . . . ensur[es] that employees do not access unapproved or superseded information." Ex. 9 at 3.

174. Counterclaim-Defendants' Accused Products also contain "*a network gateway device in communication with the computer network, the network gateway device configured to receive data in transit between a source and a destination*." For example, Webroot's DLP policies are built into Advanced Email Encryption, such that an "organization can run efficiently while protecting and monitoring sensitive information sent by [] employees." Ex. 10 at 3.



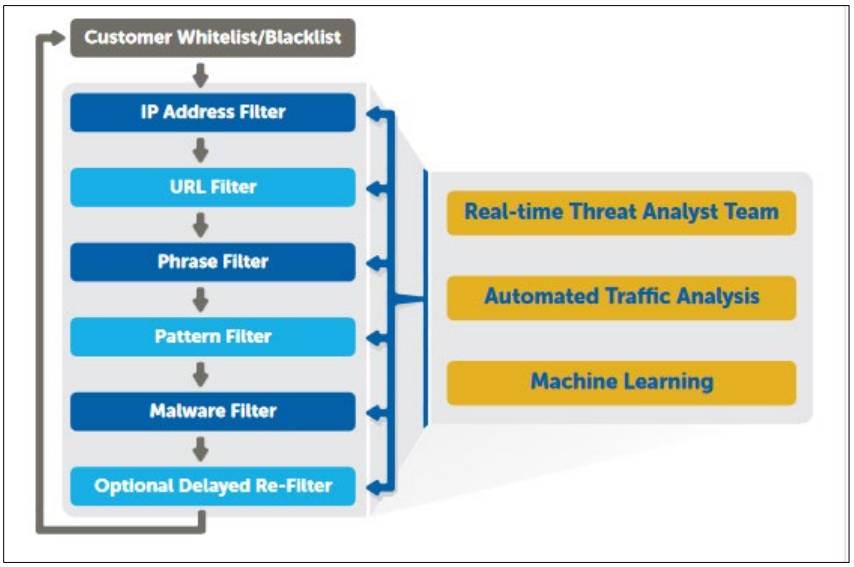
Ex. 11 at 2. OpenText's Documentum includes cloud and on-premises deployment options. Ex. 9 at 9. OpenText's Cloud Managed Services, include security and compliance options, including Webroot's Endpoint and Network Security options and Threat Intelligence Services. Ex. 12 at 1.

175. Counterclaim-Defendants' Accused Products include "*wherein the network gateway device comprises: a classification module configured to determine whether the data in transit includes prohibited content*." For example, Webroot's DLP "detect[s] information in email subject, body and attachments" and has the ability to "stop inappropriate content." Ex. 10 at 1, 2. OpenText's Documentum "seamlessly integrate[s] with existing enterprise security and identi[fies] management infrastructure, while automating security based on content attributes and user roles." Ex. 13 at 4.

176. Counterclaim-Defendants' Accused Products include "*a context information module configured to generate destination contextual information related to the destination of the received data*." For example, Webroot's DLP includes user management features (Ex. 11 at 2) and "stop[s] messages sent by unauthorized users and hold[s] for review . . . . For example, a bank teller sending financial data externally or an intern sending customer data to a personal account." Ex. 10 at 2. Likewise, OpenText's Documentum D2 "offers a configuration tool and rules engine that governs the policies and behaviors of content in OpenText Documentum." Ex. 15 at 2. For example, "OpenText Documentum Information Rights Management Services controls, secures and tracks sensitive information wherever it resides—within a workgroup, across departments and agencies or with partners and suppliers outside the firewall." Ex. 16 at 3. Additionally, Documentum provides "access to content and streamline[d] information management with personalized role-based experiences." Ex. 9 at 8. Documentum also "seamlessly integrate[s] with existing enterprise security and identif[ies] management infrastructure while automating security based on content attributes and user roles." Ex. 13 at 4.

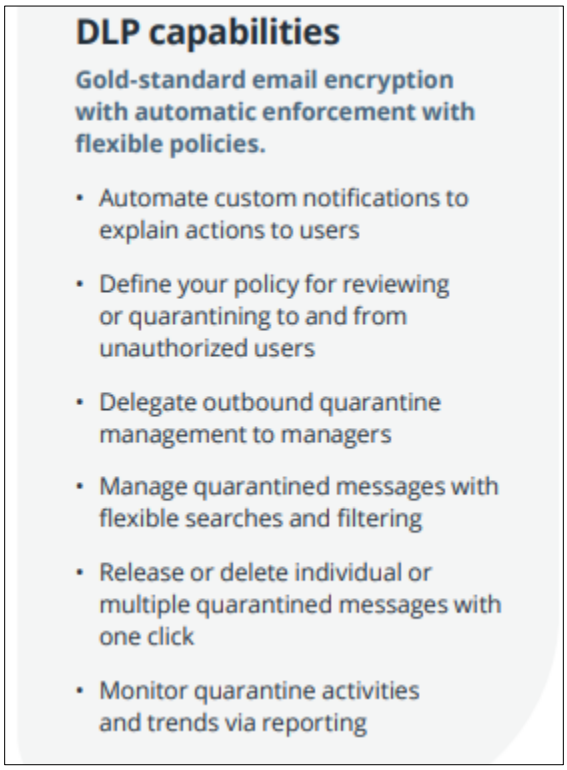
177. Counterclaim-Defendants' Accused Products include "*wherein the destination contextual information comprises a categorization of an Internet Protocol (IP) address of the*

destination, and wherein the categorization of the IP address of the destination is based at least in part on website content stored at the destination." For example, Webroot's DLP also permits various customizations for its security policies, including "blocking or whitelisting of individual URLs or IP addresses." Ex. 17 at 6. Likewise, Webroot's DLP, which runs on a single console with Zix DLP, includes a "multi-layer filtering engine . . . [and] combines standard IP address and URL filters." Ex. 18 at 2.



Id. As another example, OpenText's Documentum "provides client sessions with connection information, such as IP addresses and port numbers." Ex. 19 at 34. Additionally, "[n]etwork locations identify locations on a network, and optionally, a range of IP addresses, from which users connect to Documentum web clients." Ex. 20.

178. Counterclaim-Defendants' Accused Products also include "*a transmission policy module configured to determine a transmission policy based on the determination of the classification module and the destination contextual information*." For example, Webroot's DLP includes a number of transmission policies with "automatic enforcement." Ex. 10 at 1.



Id. In addition to those policies included in the image above, Webroot DLP also includes transmission policies to "stop messages sent by unauthorized users and hold for review . . . . For example, a bank teller sending financial data externally or an intern sending customer data to a personal account." *Id.* at 2. Likewise, OpenText's Documentum includes a "robust, fault-tolerant, cloud-ready architecture to manage and control all information content . . . [and which] scales to meet the most strenuous requirements while ensuring constant governance policies, regardless of location." Ex. 9 at 5. Additionally, OpenText's Documentum D2 "offers a configuration tool and rules engine that governs the policies and behaviors of content in OpenText Documentum as well as the interaction between content and users." Ex. 15 at 2.

179. Counterclaim-Defendants became aware of the '001 Patent at least as of the filing of Forcepoint's First Amended Answer and Counterclaims.

180. Counterclaim-Defendants actively induced and are actively inducing infringement of at least claim 1 of the ’001 Patent, in violation of 35 U.S.C. § 271(b).

181. Counterclaim-Defendants partners, customers, and end-users directly infringe at least claim 1 of the ’001 Patent, at least by using the Counterclaim-Defendants’ Accused Products.

182. Counterclaim-Defendants knowingly induce infringement of at least claim 1 of the ’001 Patent by partners, customers, and end-users of the Counterclaim-Defendants’ Accused Products with specific intent to induce infringement, and/or with willful blindness to the possibility that its acts induce infringement, through activities relating to the selling, marketing, advertising promotion, support, and distribution of the Counterclaim-Defendants’ Accused Products in the United States.

183. Counterclaim-Defendants instruct partners, customers, and end-users, at least through its marketing, promotional, and instructional materials, to use the infringing Counterclaim-Defendants’ Accused Products.

184. Counterclaim-Defendants contributed and are contributing to infringement of at least claim 1 of the ’001 Patent, in violation of 35 U.S.C. § 271(c) by making, using, offering to sell, selling, and importing the Counterclaim-Defendants’ Accused Products and/or components thereof which constitute material parts of the claimed inventions of the ’001 Patent and have no substantial non-infringing uses.

185. Counterclaim-Defendants’ infringement of the ’001 Patent has been knowing and willful since at least the filing of Forcepoint’s First Amended Answer and Counterclaims.

186. Counterclaim-Defendants’ continued infringement of the ’001 Patent has damaged and will continue to damage Forcepoint.

187. Unless and until enjoined by this Court, Counterclaim-Defendants will continue to directly infringe as well as induce and contribute to infringement of the '001 Patent. Counterclaim-Defendants' infringing acts are causing and will continue to cause at least Forcepoint irreparable harm, for which there is no adequate remedy at law. Under 35 U.S.C. § 283, Forcepoint is entitled to a permanent injunction against further infringement.

COUNTERCLAIM XV
(INFRINGEMENT OF U.S. PATENT NO. 9,654,495)

188. Forcepoint realleges and incorporates by reference the allegations set forth in the foregoing paragraphs.

189. Counterclaim-Defendants' products and/or services that infringe the '495 Patent include, but are not limited to, the Counterclaim-Defendants' Accused Products and use thereof.

190. Counterclaim-Defendants make, use, sell, offer for sale, and/or import the Counterclaim-Defendants' Accused Products and components thereof in the United States.

191. Counterclaim-Defendants have infringed, either literally or under the doctrine of equivalents, and continue to infringe one or more claims of the '495 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. Forcepoint will continue to suffer irreparable harm unless this Court enjoins Counterclaim-Defendants, their agents, employees, representatives, and all others acting in concert with Counterclaim-Defendants from infringing the '495 Patent.

192. Counterclaim-Defendants' Accused Products practice one or more of the '495 Patent's claims. For example, Counterclaim-Defendants' Accused Products, including but not limited to Webroot DNS Protection, practice each element of at least claim 1 of the '495 Patent as demonstrated below.

193. For example, claim 1 of the '495 Patent recites:

> A method of controlling access to requested web content, implemented on at least one processor, comprising:
>
> receiving, using at least the processor, a request for access to web content located at an address specified by a uniform resource locator (URL);
>
> determining which processes are spawned by the web content identified by the URL;
>
> comparing which processes are spawned with a list to determine properties of the URL; and
>
> determining, using at least the processor, whether to allow the request based at least partly on the determined properties.

194. To the extent the preamble is limiting, Counterclaim-Defendants' Accused Products perform "*[a] method of controlling access to requested web content, implemented on at least one processor*." For example, DNS Protection "aim[s] to create a highly secure, private, resilient and manageable connection to the internet." Ex. 22 (https://www.webroot.com/us/en/business/dns-protection) at 1. DNS Protection also includes "[a]utomated filtering us[ing] Webroot BrightCloud® Internet Threat Intelligence to automatically block requests to undesirable, dangerous or malicious internet domains, even encrypted DNS over HTTPS (DoH) requests." *Id.* As the figures below show, DNS Protection employs various methods to block domains and filter web content.

Webroot® DNS Protection and NSA/CISA PDNS service attributes

The NSA and CISA advisory recommends the following attributes of a protective DNS service:

Attributes	Webroot	Method
Blocks malware domains	Yes	Using Webroot BrightCloud® Threat Intelligence
Blocks phishing domains	Yes	Using Webroot BrightCloud® Threat Intelligence
Malware Domain Generation Algorithm (DGA) protection	Yes	Using Webroot BrightCloud® Threat Intelligence
Leverages machine learning or other heuristics to augment threat feeds	Yes	Uses the Webroot ML/AI platform established in 2007
Content filtering	Yes	Uses up to 80 URL categories, plus Google SafeSearch
Supports API access for SIEM integration or custom analytics	Yes	Several options for ensuring full logging and visibility of requests with ingestion into SIEM, XDR, MDR, etc.
Web interface dashboard	Yes	Webroot's new UI/UX makes policy management, reporting and dashboard stats always available
Validates DNSSEC	Yes	Webroot uses DNSSEC
DoH/DoT capable	Yes	DoH is uniquely supported natively and is also GDPR compliant where necessary.
Enables customizable policies by group, device or network	Yes	Comprehensive management controls exist and coverage of both the network and guest WiFi requests
Deploys across hybrid architectures	Yes	We support hybrid architectures

Id. at 1-2. FAQs regarding Webroot® DNS Protection describe it as "a SaaS security solution that harnesses the domain name system (DNS) to securely filter all outbound DNS requests and secure DNS connections to the internet. It automatically filters all DNS requests to stop traffic going to, and responding from, domains known to be security risks." Ex. 23 (https://www-cdn.webroot.com/4815/9370/2622/Webroot_DoH_DNS_FAQ.pdf) at 1. Webroot DNS protection also "selectively control[s] internet access." See (https://vimeo.com/386841417?gclid=CjwKCAjwnZaVBhA6EiwAVVyv9JyhKipRdE815E-sxxs9Lfu9oeFokpvsk9TYastLCadrqRSOrwKJAxoCBbgQAvD_BwE) at 1:01.

195. Counterclaim-Defendants' Accused products also include "*receiving, using at least the processor, a request for access to web content located at an address specified by a uniform resource locator (URL)*." For example, by using Webroot® DNS Protection "organizations control their networks and maintain the security, privacy and visibility they need

to protect IT infrastructure and users, even those working remotely." Webroot® DNS protection also supports "both IPv6 and DoH so businesses are prepared for the next generation of internet protocols and requests." Ex. 22 at 2. Additionally, "Webroot® DNS Protection works by managing the DNS requests of the network and individual systems. These requests, regardless of whether they are traditional clear text or new, encrypted DNS over HTTPS (DoH) requests, are sent directly to [Webroot's] hardened and secured DNS resolver servers." Ex. 23 at 1. These resolver servers "are hosted at the heart of the internet, in highly secure Google Cloud™ datacenters[.]" *Id.* Webroot DNS Protection "maximize[s] security" with Webroot BrightCloud® Threat Intelligence Services, which "provide the essential threat data for Webroot® DNS Protection. This includes the identification of alternate DoH resolvers. These are automatically filtered, essentially preventing applications from making independent or rogue DNS requests. . . . In terms of URL categorization, Webroot improves accuracy by assigning a confidence level to [its] categorizations." *Id.* at 2.

196. Counterclaim-Defendants' Accused products also include "*determining which processes are spawned by the web content identified by the URL*." For example, as the figure below shows, Webroot® DNS Protection incorporates Webroot BrightCloud® Threat Intelligence for various functions, including but not limited to, blocking malware and phishing domains.

Webroot® DNS Protection and NSA/CISA PDNS service attributes

The NSA and CISA advisory recommends the following attributes of a protective DNS service:

Attributes	Webroot	Method
Blocks malware domains	Yes	Using Webroot BrightCloud® Threat Intelligence
Blocks phishing domains	Yes	Using Webroot BrightCloud® Threat Intelligence
Malware Domain Generation Algorithm (DGA) protection	Yes	Using Webroot BrightCloud® Threat Intelligence
Leverages machine learning or other heuristics to augment threat feeds	Yes	Uses the Webroot ML/AI platform established in 2007
Content filtering	Yes	Uses up to 80 URL categories, plus Google SafeSearch
Supports API access for SIEM integration or custom analytics	Yes	Several options for ensuring full logging and visibility of requests with ingestion into SIEM, XDR, MDR, etc.
Web interface dashboard	Yes	Webroot's new UI/UX makes policy management, reporting and dashboard stats always available
Validates DNSSEC	Yes	Webroot uses DNSSEC
DoH/DoT capable	Yes	DoH is uniquely supported natively and is also GDPR compliant where necessary.
Enables customizable policies by group, device or network	Yes	Comprehensive management controls exist and coverage of both the network and guest WiFi requests
Deploys across hybrid architectures	Yes	We support hybrid architectures

Ex. 22 at 1-2. Webroot BrightCloud® Threat Intelligence "provide content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites." Ex. 6 at 1. "It determines whether the site poses a phishing risk at the precise moment it is encountered, meaning the analysis and determinations are never stale." *Id.* at 2. Webroot BrightCloud® Threat Intelligence was "[d]esigned to combat polymorphic malware," which "allows [its] partners' device to make determinations at the network level to enable users to quickly allow, block or flag files for investigation." *Id.* Furthermore, BrightCloud can "predict how likely an internet object is to be malicious" based on its "associations with other URLs, IPs, files and mobile apps." *Id.*

197. Counterclaim-Defendants' Accused products also include "*comparing which processes are spawned with a list to determine properties of the URL*." For example, BrightCloud® Threat Intelligence Services "provide content classification and independent

reputation scores for billions of webpages to keep end users from visiting unwanted and unsafe sights." *Id.* at 1. Using the "contextual analysis engine" BrightCloud® Threat Intelligence Services "takes disparate data from BrightCloud Platform feeds and correlates it for deep insight into the landscape of interconnected URLs, IPs, files and mobile apps." *Id.* at 2. Additionally, IP Reputation Service provides "a dynamic list of millions of malicious IPs at any given time to block malicious traffic from entering a network." Ex. 14 (https://www-cdn.webroot.com/5815/6038/0066/BrightCloud_Threat_Intelligence_Services_Overview_Datasheet_us.pdf) at 2. And File Reputation Service provides a "continuously updated real-time lookup service of billions of known malicious and white-listed file identifiers" to provide "dynamic file reputation information to enable security resources to focus on the most pressing threats." *Id.*

198. Counterclaim-Defendants' Accused products also include "*determining, using at least the processor, whether to allow the request based at least partly on the determined properties*." For example, Webroot® DNS Protection can "automatically block requests to undesirable, dangerous or malicious internet domains . . . ." Ex. 22 at 1. Further, "[a]ll DNS requests are filtered." Ex. 24 (https://www-cdn.webroot.com/5915/9432/4948/Webroot_DNS_Protection_DS.pdf) at 2. And "[b]y securely filtering all DNS requests for high-risk domains, businesses drastically reduce their exposure to threats." *Id.* . And as the figure below shows, Webroot® DNS Protection "stop[s] malicious inbound web traffic and threats."

Ex. 25 (https://www.webroot.com/us/en/business/dns-protection/off-network-protection) at 3. Further, IP Reputation Service can "block malicious traffic from entering a network." Ex. 14 at 2. Streaming Malware Detection allows Webroot's partners' devices "to make determinations at the network level to enable users to quickly allow, block or flag files for investigation." Ex. 6 at 2. Similarly Real-Time Anti-Phishing Service "provides effective, live protection against zero-hour phishing attacks . . . ." *Id.*

199. Counterclaim-Defendants became aware of the '495 Patent at least as of the filing of Forcepoint's First Amended Answer and Counterclaims.

200. Counterclaim-Defendants actively induced and are actively inducing infringement of at least claim 1 of the '495 Patent, in violation of 35 U.S.C. § 271(b).

201. Counterclaim-Defendants' partners, customers, and end-users directly infringe at least claim 1 of the '495 Patent, at least by using the Counterclaim-Defendants' Accused Products.

202. Counterclaim-Defendants knowingly induce infringement of at least claim 1 of the '495 Patent by partners, customers, and end-users of the Counterclaim-Defendants' Accused Products with specific intent to induce infringement, and/or with willful blindness to the

possibility that its acts induce infringement, through activities relating to the selling, marketing, advertising promotion, support, and distribution of the Counterclaim-Defendants' Accused Products in the United States.

203. Counterclaim-Defendants instruct partners, customers, and end-users, at least through its marketing, promotional, and instructional materials, to use the infringing Counterclaim-Defendants' Accused Products.

204. Counterclaim-Defendants contributed and are contributing to infringement of at least claim 1 of the '495 Patent, in violation of 35 U.S.C. § 271(c) by making, using, offering to sell, selling, and importing the Counterclaim-Defendants' Accused Products and/or components thereof which constitute material parts of the claimed inventions of the '495 Patent and have no substantial non-infringing uses.

205. Counterclaim-Defendants' infringement of the '495 Patent has been knowing and willful since at least the filing of Forcepoint's First Amended Answer and Counterclaims.

206. Counterclaim-Defendants' continued infringement of the '495 Patent has damaged and will continue to damage Forcepoint.

207. Unless and until enjoined by this Court, Counterclaim-Defendants will continue to directly infringe as well as induce and contribute to infringement of the '495 Patent. Counterclaim-Defendants' infringing acts are causing and will continue to cause at least Forcepoint irreparable harm, for which there is no adequate remedy at law. Under 35 U.S.C. § 283, Forcepoint is entitled to a permanent injunction against further infringement.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Forcepoint hereby respectfully requests a jury trial on all issues and claims so triable.

PRAYER FOR RELIEF

WHEREFORE, Forcepoint requests the following judgments and seeks the following relief:

(i) That all claims against Forcepoint be dismissed with prejudice and that all relief requested by Plaintiffs be denied;

(ii) That a judgment be entered declaring that Forcepoint has not infringed and does not infringe, either directly or indirectly, any valid and enforceable claim of the Asserted Patents, either literally or under the doctrine of equivalents;

(iii) That a judgment be entered declaring that the claims of the Asserted Patents are invalid and/or unenforceable for failure to comply with the statutory provisions of Title 35 of the United States Code, including without limitation, one or more of §§ 101, 102, 103, and/or 112;

(iv) That a judgment be entered in favor of Forcepoint against Counterclaim-Defendants on Forcepoint's Counterclaims;

(v) That the Court find that Counterclaim-Defendants willfully infringes, directly and indirectly, the Asserted Counterclaim Patents;

(vi) That the Court permanently enjoin Counterclaim-Defendants, their affiliates and subsidiaries, and each of their officers, agents, servants and employees and those acting in privity or concert with them, from making, offering to sell, selling, using, or importing into the United States products claimed in any of the claims of the Asserted Counterclaim Patents;

(vii) That the Court award damages under 35 U.S.C. §§ 154 & 284 in an amount sufficient to compensate Forcepoint for its damages arising from infringement by

Counterclaim-Defendants, including, but not limited to, lost profits and/or a reasonable royalty, and an accounting;

(viii) That the Court require Counterclaim-Defendants to pay Forcepoint the prejudgment and post-judgment interest to the fullest extent allowed under the law;

(ix) That the Court award Forcepoint its costs as the prevailing party;

(x) That a judgment be entered declaring that this case is exceptional under 35 U.S.C. § 285, and accordingly that Forcepoint is entitled to recover reasonable attorneys' fees and costs on prevailing in this action; and

(xi) That Forcepoint be awarded such other relief that the Court deems just and proper.

Dated: July 14, 2022

Respectfully submitted,

/s/ Kat Li

Kat Li
Texas State Bar No. 24070142
kat.li@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
United States
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Adam R. Alper (*pro hac vice pending*)
aalper@kirkland.com
Akshay S. Deoras (*pro hac vice pending*)
adeoras@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, CA 94104
United States
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Michael W. De Vries (*pro hac vice pending*)
michael.devries@kirkland.com
KIRKLAND & ELLIS LLP
555 South Flower Street
Los Angeles, CA 90071
United States
Telephone: (213) 680-8400
Facsimile: (213) 680-8500

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service are being served on July 14, 2022 with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ Kat Li
Kat Li